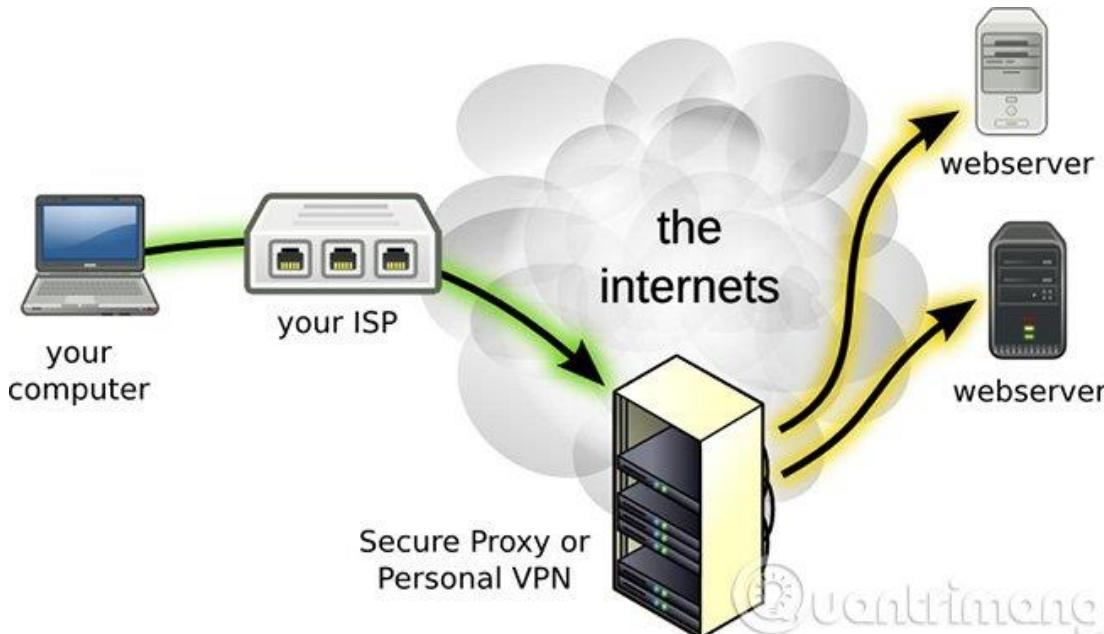


PHẦN 1 : GIỚI THIỆU VỀ VPN,L2TP,IPSEC

1.Giới thiệu về mạng riêng ảo VPN(Virtual Private Network)

1.1 Mạng riêng ảo VPN là gì ?

Mạng riêng ảo VPN - từ viết tắt của Virtual Private Network, dịch ra tiếng Việt là hệ thống mạng cá nhân ảo. Đây được hiểu là 1 hệ thống mạng, có khả năng tạo ra 1 kết nối dựa trên hệ thống mạng Public, mạng Internet... dựa trên nhà cung cấp dịch vụ nào đó



Hình 1.1 Mô hình mạng VPN

Một hệ thống VPN có thể kết nối được nhiều site khác nhau, dựa trên khu vực, diện tích địa lý... tương tự như chuẩn Wide Area Network (WAN). Bên cạnh đó, VPN còn được dùng để "khuếch tán", mở rộng các mô hình Intranet nhằm truyền tải thông tin, dữ liệu tốt hơn.

Mạng riêng ảo VPN dành riêng để kết nối các máy tính lại với nhau thông qua mạng Internet công cộng. Những máy tính tham gia mạng riêng ảo sẽ nhìn thấy nhau như trong một mạng nội bộ - LAN (Local Area Network). Internet là một môi trường công cộng, việc chia sẻ dữ liệu có tính riêng tư thông qua Internet là cực kỳ nguy hiểm vì những dữ liệu đó có thể dễ dàng bị rò rỉ, bị ăn cắp... Mạng riêng ảo là giao thức trợ giúp việc kết nối các máy tính lại với nhau thông qua một kênh truyền dẫn dữ liệu (tunel) riêng đã được mã hóa.

Mạng riêng ảo giúp bảo vệ dữ liệu trong khi chúng được truyền trên Internet. Vì vậy mạng riêng ảo thường được ứng dụng trong các trường hợp sau:

- Làm việc từ xa: Truy cập từ xa thông qua Internet vào mạng của công ty để chia sẻ dữ liệu cũng như thực thi các ứng dụng nội bộ.

- Kết nối nhiều mạng với nhau (Site-to-Site): Nếu công ty có nhiều văn phòng, việc kết nối các mạng lại với nhau thành một mạng thống nhất sẽ đem lại hiệu quả ánh tượng trong việc quản lý & chia sẻ thông tin.
- Tạo phiên làm việc an toàn: Mạng riêng ảo là giải pháp tốt & với chi phí thấp cho một số công việc đòi hỏi tính bảo mật cao như quản trị máy chủ, website, cơ sở dữ liệu...

1.2. Phân loại mạng riêng ảo

- Remote Access VPNs
- Intranet VPNs
- Extranet VPNs

1.3 Các giao thức thường dùng trong VPN

Có bốn giao thức đường hầm (tunneling protocols) phổ biến thường được sử dụng trong VPN, mỗi một trong chúng có ưu điểm và nhược điểm riêng. Chúng ta sẽ xem xét và so sánh chúng dựa trên mục đích mà sử dụng cho phù hợp :

- Internet Protocol Security (IPSec)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer2 Tunneling Protocol (L2TP)
- Secure Socket Layer (SSL)

Trong Lab này sẽ đi sâu nghiên cứu về 2 giao thức L2TP và IPSec và áp dụng thực tế của 2 giao thức này trên Windows Server 2008.

2. Giao thức L2TP (Layer 2 tunneling protocol)

2.1 Khái niệm

Giao thức Layer 2 Tunneling Protocol (L2TP) là giao thức kết hợp các đặc điểm của 2 giao thức có trước là PPTP và giao thức Layer 2 Forwarding (L2F).

Giống như PPTP, L2TP là giao thức đường hầm, nó sử dụng tiêu đề đóng gói riêng cho việc truyền các gói ở lớp 2. Một điểm khác biệt chính giữa L2F và PPTP là L2F không phụ thuộc vào IP và GRE, cho phép nó có thể làm việc ở môi trường vật lý khác. Bởi vì GRE không sử dụng như giao thức đóng gói, nên L2F định nghĩa riêng cách thức các gói được điều khiển trong môi trường khác. Nhưng nó cũng hỗ trợ TACACS+ và RADIUS cho việc xác thực. Có hai mức xác thực người dùng: Đầu tiên ở ISP trước khi thiết lập đường hầm, Sau đó là ở cổng nối của mạng riêng sau khi kết nối được thiết lập.

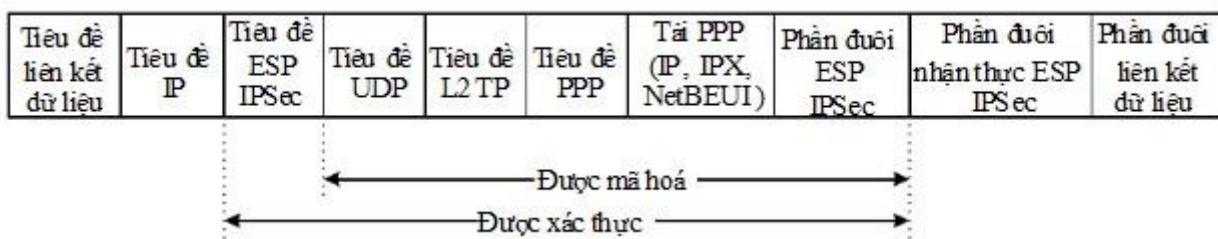
L2TP mang đặc tính của PPTP và L2F. Tuy nhiên, L2TP định nghĩa riêng một giao thức đường hầm dựa trên hoạt động của L2F. Nó cho phép L2TP truyền thông qua nhiều môi trường gói khác nhau như X.25, Frame Relay, ATM. Mặc dù nhiều công cụ chủ yếu của L2TP tập trung cho UDP của mạng IP, nhưng có thể thiết lập một hệ thống L2TP mà không cần phải sử dụng IP làm giao thức đường hầm. Một mạng ATM hay frame Relay có thể áp dụng cho đường hầm L2TP.

Do L2TP là giao thức ở lớp 2 nên nó cho phép người dùng sử dụng các giao thức điều khiển một cách mềm dẻo không chỉ là IP mà có thể là IPX hoặc NETBEUI. Cũng giống như PPTP, L2TP cũng có cơ chế xác thực PAP, CHAP hay RADIUS.

L2TP yêu cầu sử dụng chứng chỉ số (digital certificates). Xác thực người dùng có thể được thực hiện thông qua cùng cơ chế xác thực PPP tương tự như PPTP.

L2TP có một vài ưu điểm so với PPTP. PPTP cho bạn khả năng bảo mật dữ liệu, nhưng L2TP còn tiến xa hơn khi cung cấp thêm khả năng đảm bảo tính toàn vẹn dữ liệu (bảo vệ chống lại việc sửa đổi dữ liệu trong khoảng thời gian nó di chuyển từ người gửi đến người nhận, khả năng xác thực nguồn gốc (xác định người dùng đã gửi dữ liệu có thực sự đúng người), và khả năng bảo vệ chống gửi lại – replay protection (chống lại việc hacker chặn dữ liệu đã được gửi, ví dụ thông tin quyền đăng nhập (credentials), rồi sau đó gửi lại (replay) chính thông tin đó để bẫy máy chủ. Một khác, do liên quan đến cung cấp các khả năng bảo mật mở rộng làm cho L2TP chạy chậm hơn chút ít so với PPTP.

2.2 Cấu trúc gói L2TP



Hình 1.2 Cấu trúc gói L2TP

❖ Đóng gói L2TP

Phần tải PPP ban đầu được đóng gói với một PPP header và một L2TP header.

❖ Đóng gói UDP

Gói L2TP sau đó được đóng gói với một UDP header, các địa chỉ nguồn và đích được đặt bằng 1701.

❖ Đóng gói IPSec

Tùy thuộc vào chính sách IPSec, gói UDP được mã hóa và đóng gói với ESP IPSec header và ESP IPSec Trailer

❖ Đóng gói IP

Gói IPSec được đóng gói với IP header chứa địa chỉ IP nguồn và đích của VPN client và VPN server.

❖ Đóng gói lớp liên kết dữ liệu

Do đường hầm L2TP hoạt động ở lớp 2 của mô hình OSI- lớp liên kết dữ liệu nên các IP datagram cuối cùng sẽ được đóng gói với phần header và trailer tương ứng với kỹ thuật ở lớp đường truyền dữ

liệu của giao diện vật lý đầu ra. Ví dụ, khi các IP datagram được gửi vào một giao diện Ethernet thì IPdatagram này sẽ được đóng gói với Ethernet header và Ethernet Trailer. Khi các IP datagram được gửi trên đường truyền WAN điểm-tới-điểm (chẳng hạn đường dây điện thoại hay ISDN,) thì IPdatagram được đóng gói với PPP header và PPP trailer.

2.3.Ưu nhược điểm của L2TP

a.Uu điểm

- Người dùng khai thác ưu điểm giá rẻ của Internet.Thay vì phải thực hiện cuộc gọi đường dài để kết nối trực tiếp đến máy chủ truy cập từ xa của một nơi, người dùng chỉ cần gọi đến số IP cục bộ và dùng Internet để xử lý các kết nối đường dài
- Giao thức cung cấp dial ảo vì người dùng thực tế không gọi đến nơi đó ,nhưng khi kết nối xong nó có vẻ như là dial up.
- Vì có dùng tạo khung PPP,người dùng từ xa có thể truy cập đến các nơi bằng nhiều giao thức như IP,IPX,SNA,....
- L2TP cung cấp các hệ đầu cuối có tính trong suốt ,nghĩa là người dùng từ xa và nơi truy cập không yêu cầu phần mềm đặc biệt để sử dụng dịch vụ một cách an toàn.
- L2TP cung cấp giải pháp truyền dữ liệu an toàn khi sử dụng IP Sec để mã hóa và sau đó dùng IPSec để xác thực đối với từng gói tin nhận được

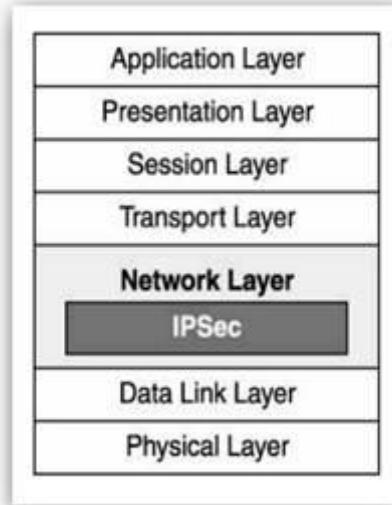
b.Nhược điểm

- L2TP chạy chậm hơn so với cả PPTP lẫn L2F bởi vì nó sử dụng IPSec để xác thực mỗi gói tin nhận được
- Mặc dù L2TP đã có tất cả các đặc tính của PPTP một máy chủ truy cập xa RRAS vẫn cần phải cấu hình thêm khi chạy trên L2TP.

3. Giao thức bảo mật IP Sec (Internet Protocol Security)

3.1 Định nghĩa

IP Security (IPSec) là một giao thức được chuẩn hoá bởi IETF từ năm 1998 nhằm mục đích nâng cấp các cơ chế mã hoá và xác thực thông tin cho chuỗi thông tin truyền đi trên mạng bằng giao thức IP. Hay nói cách khác, IPSec là sự tập hợp của các chuẩn mở được thiết lập để đảm bảo sự cẩn mật dữ liệu, đảm bảo tính toàn vẹn dữ liệu và chứng thực dữ liệu giữa các thiết bị mạng.



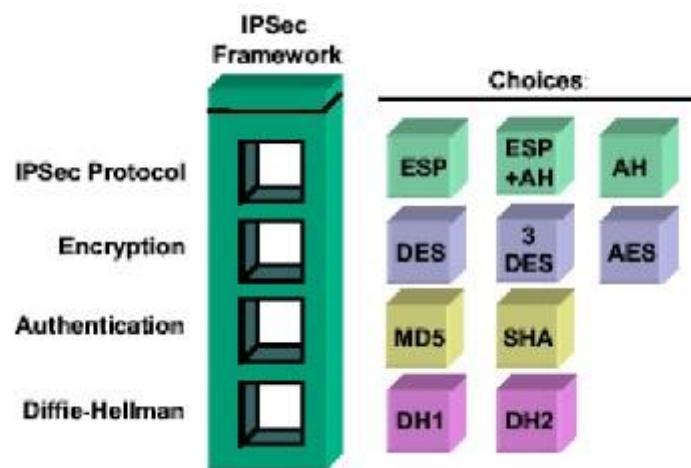
Hình 3.1 Vị trí IPSec trong mô hình OSI

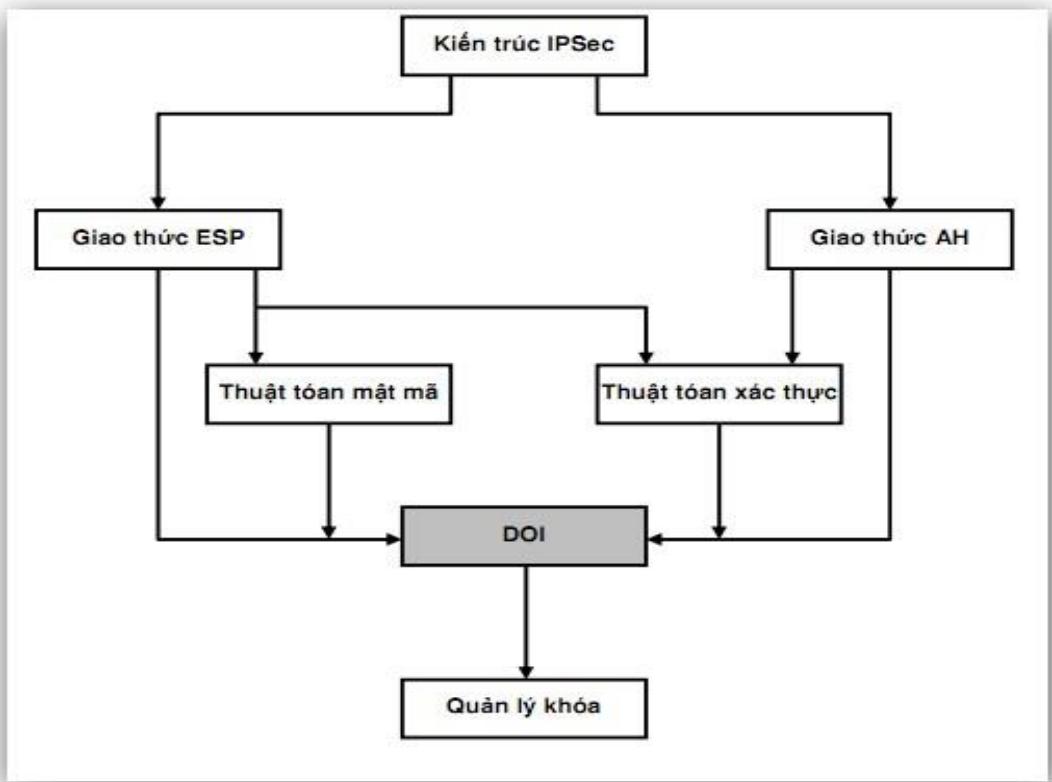
IPSec cung cấp một cơ cấu bảo mật ở tầng 3 (Network layer) của mô hình OSI.

IPSec được thiết kế như phần mở rộng của giao thức IP, được thực hiện thống nhất trong cả hai phiên bản IPv4 và IPv6. Đối với IPv4, việc áp dụng IPSec là một tùy chọn, nhưng đối với IPv6, giao thức bảo mật này được triển khai bắt buộc.

3.2 Kiến trúc IPSec

IPSec là một giao thức phức tạp, dựa trên nền của nhiều kỹ thuật cơ sở khác nhau như mật mã, xác thực, trao đổi khoá... Xét về mặt kiến trúc, IPSec được xây dựng dựa trên các thành phần cơ bản sau đây, mỗi thành phần được định nghĩa trong một tài liệu riêng tương ứng :





Hình 3.2 Kiến trúc IPSec

- Kiến trúc IPSec (RFC 2401): Quy định các cấu trúc, các khái niệm và yêu cầu của IPSec.
- Giao thức ESP (RFC 2406): Mô tả giao thức ESP, là một giao thức mật mã và xác thực thông tin trong IPSec.
- Giao thức AH (RFC 2402): Định nghĩa một giao thức khác với chức năng gần giống ESP. Như vậy khi triển khai IPSec, người sử dụng có thể chọn dùng ESP hoặc AH, mỗi giao thức có ưu và nhược điểm riêng.
- Thuật toán mật mã: Định nghĩa các thuật toán mã hoá và giải mã sử dụng trong IPSec. IPSec chủ yếu dựa vào các thuật toán mã hoá đối xứng. Thuật toán thường sử dụng DES, 3DES.
- Thuật toán xác thực: Định nghĩa các thuật toán xác thực thông tin sử dụng trong AH và ESP. Sử dụng RSA, RSA Encrypted Nonces.
- Quản lý khoá (RFC 2408): Mô tả các cơ chế quản lý và trao đổi khoá trong IPSec. Thường sử dụng DH, CA
- Miền thực thi (Domain of Interpretation – DOI): Định nghĩa môi trường thực thi IPSec. IPSec không phải là một công nghệ riêng biệt mà là sự tổ hợp của nhiều cơ chế, giao thức và kỹ thuật khác nhau, trong đó mỗi giao thức, cơ chế đều có nhiều chế độ hoạt động khác nhau. Việc xác định một tập các chế độ cần thiết để triển khai IPSec trong một tình huống cụ thể là chức năng của miền thực thi. Xét về mặt ứng dụng, IPSec thực chất là một giao thức hoạt động song song với IP nhằm cung cấp 2 chức năng cơ bản mà IP nguyên thuỷ chưa có, đó là mã hoá và xác thực gói dữ liệu. Một cách khái quát có thể xem IPSec là một tổ hợp gồm hai thành phần:
 - ✓ Giao thức đóng gói, gồm AH và ESP

- ✓ Giao thức trao đổi khoá IKE (Internet Key Exchange)

3.3 Các dịch vụ của IPSec

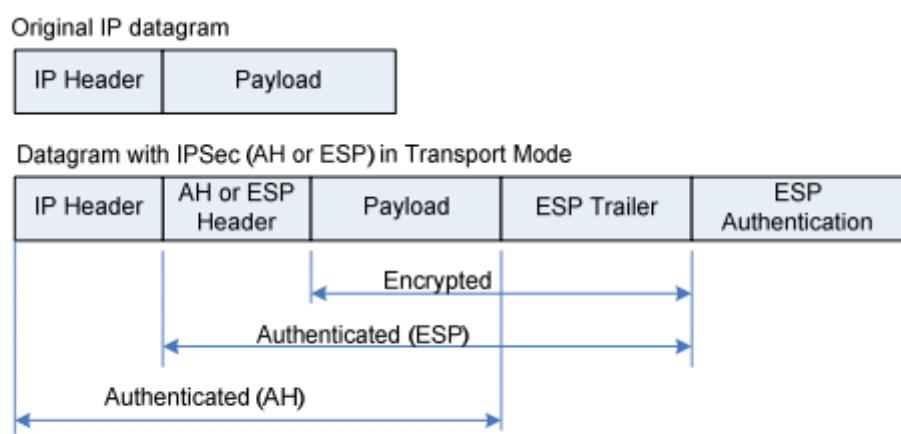
- Quản lý truy xuất (access control)
- Toàn vẹn dữ liệu ở chế độ không kết nối (connectionless integrity)
- Xác thực nguồn gốc dữ liệu (data origin authentication)
- Chống phát lại (anti-replay)
- Mã hoá dữ liệu (encryption)
- Bảo mật dòng lưu lượng (traffic flow confidentiality)

Việc cung cấp các dịch vụ này trong từng tình huống cụ thể phụ thuộc vào giao thức đóng gói được dùng là AH hay ESP. Theo đó nếu giao thức được chọn là AH thì các dịch vụ mã hoá và bảo mật dòng dữ liệu sẽ không được cung cấp.

3.4 Các chế độ Transport Mode hoạt động của IPSec

- Transport Mode (chế độ vận chuyển)

Transport mode cung cấp cơ chế bảo vệ cho dữ liệu của các lớp cao hơn (TCP, UDP hoặc ICMP). Trong Transport mode, phần IPSec header được chèn vào giữa phần IP header và phần header của giao thức tầng trên, như hình mô tả bên dưới, AH và ESP sẽ được đặt sau IP header nguyên thủy. Vì vậy chỉ có tải (IP payload) là được mã hóa và IP header ban đầu là được giữ nguyên vẹn. Transport mode có thể được dùng khi cả hai host hỗ trợ IPSec. Chế độ transport này có thuận lợi là chỉ thêm vào vài bytes cho mỗi packets và nó cũng cho phép các thiết bị trên mạng thấy được địa chỉ đích cuối cùng của gói. Khả năng này cho phép các tác vụ xử lý đặc biệt trên các mạng trung gian dựa trên các thông tin trong IP header. Tuy nhiên các thông tin Layer 4 sẽ bị mã hóa, làm giới hạn khả năng kiểm tra của gói.



IPSec Transport-mode – a generic representation

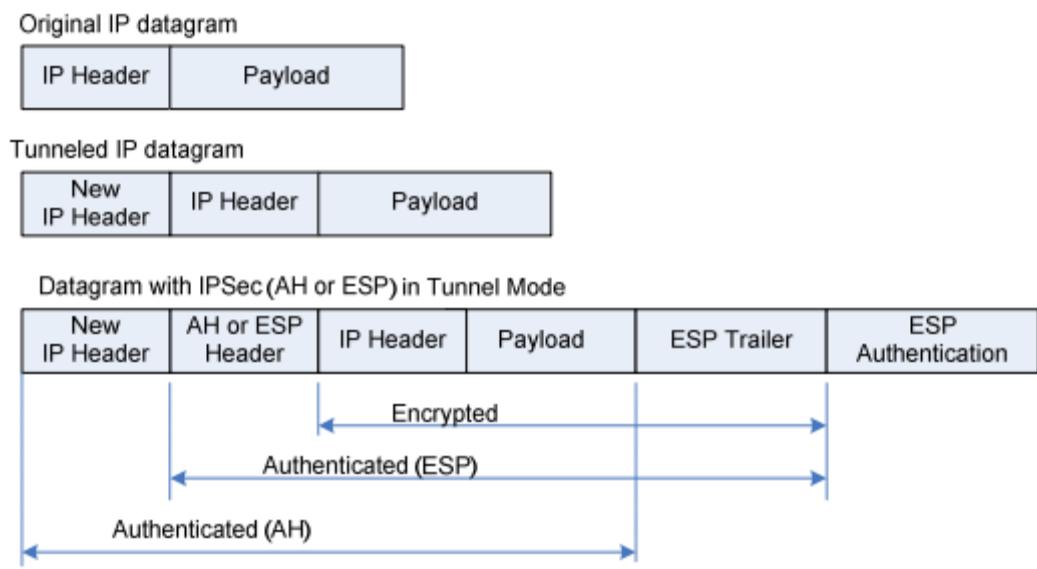
Hình 3.5.1 IPSec Transport mode

- Tunnel mode (Chế độ đường hầm)

- ✓ Không giống Transport mode, Tunnel mode bảo vệ toàn bộ gói dữ liệu. Toàn bộ gói dữ liệu IP được đóng gói trong một gói dữ liệu IP khác và một IPSec header được chèn vào giữa phần đầu nguyên bản và phần đầu mới của IP. Toàn bộ gói IP ban đầu sẽ bị đóng

gói bởi AH hoặc ESP và một IP header mới sẽ được bao bọc xung quanh gói dữ liệu. Toàn bộ các gói IP sẽ được mã hóa và trở thành dữ liệu mới của gói IP mới. Chế độ này cho phép những thiết bị mạng, chẳng hạn như router, hoạt động như một IPSec proxy thực hiện chức năng mã hóa thay cho host. Router nguồn sẽ mã hóa các packets và chuyển chúng dọc theo tunnel. Router đích sẽ giải mã gói IP ban đầu và chuyển nó về hệ thống cuối. Vì vậy header mới sẽ có địa chỉ nguồn chính là gateway.

- ✓ Với tunnel hoạt động giữa hai security gateway, địa chỉ nguồn và đích có thể được mã hóa. Tunnel mode được dùng khi một trong hai đầu của kết nối IPSec là security gateway và địa chỉ đích thật sự phía sau các gateway không có hỗ trợ IPSec.



Hình 3.5.2 IPSec Tunnel mode

3.5 Ưu điểm và khuyết điểm của IPSec

a. Ưu điểm

- Khi IPSec được triển khai trên bức tường lửa hoặc bộ định tuyến của một mạng riêng, thì tính năng an toàn của IPSec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan đến bảo mật.
- IPSec được thực hiện bên dưới lớp TCP và UDP, đồng thời nó hoạt động trong suốt đối với các lớp này. Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi IPSec được triển khai.
- IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối, điều này giúp che giấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua mạng Internet.

b. Hạn chế

- Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kỹ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
- IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
- Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

PHẦN 2 : LAB CẤU HÌNH L2TP/IPSEC TRÊN WINDOWS SERVER 2012

Trong phần này sẽ đi vào thực hành để hiểu về ứng dụng thực tế của L2TP/IPSec qua 2 phương thức sử dụng khác nhau là :

- ❖ VPN Client to site sử dụng giao thức L2TP Preshared Key
- ❖ VPN L2TP/IPSEC sử dụng Certificate

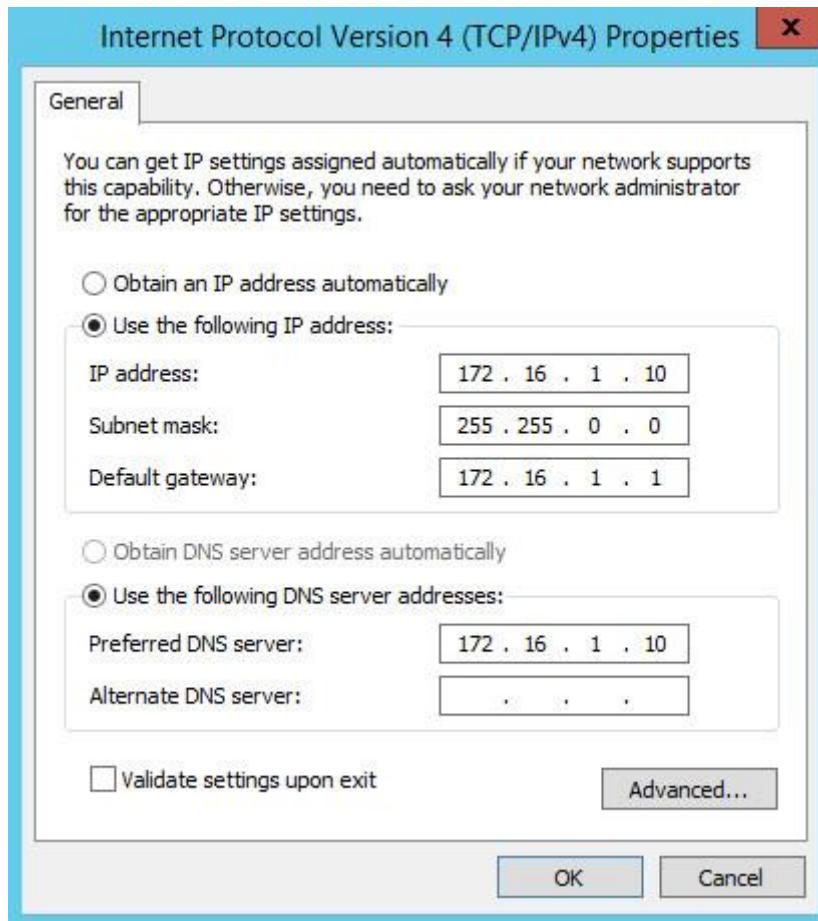
1.VPN client to site sử dụng giao thức L2TP preshared key

Để thực hiện bài lap này ta cần chuẩn bị:

- Một máy Windowserver 2012 làm DC đã nâng Domain mangmaytinh.com
- Một máy Windowserver 2012 làm VPN server đã join domain mangmaytinh.com
- Một máy window 7 làm VPN client

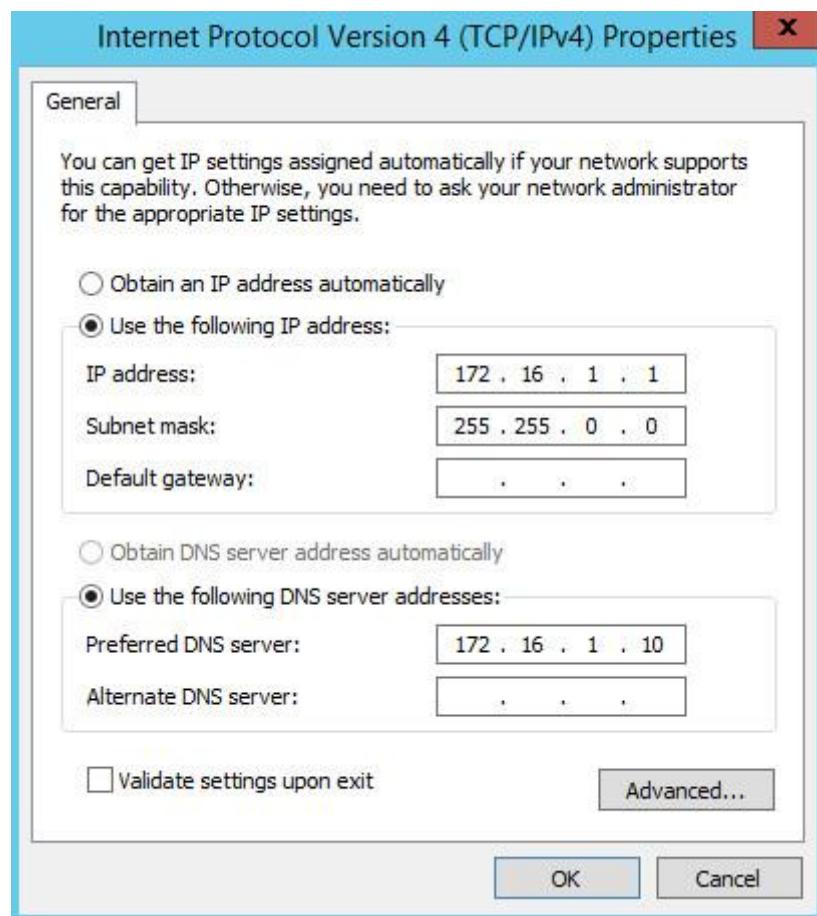
Bước 1: Đặt địa chỉ IP và card mạng(trên VMWare) cho các máy

Máy DC: có 1 card mạng ta để ở Vmnet0 (trong VMWare) địa chỉ IP là

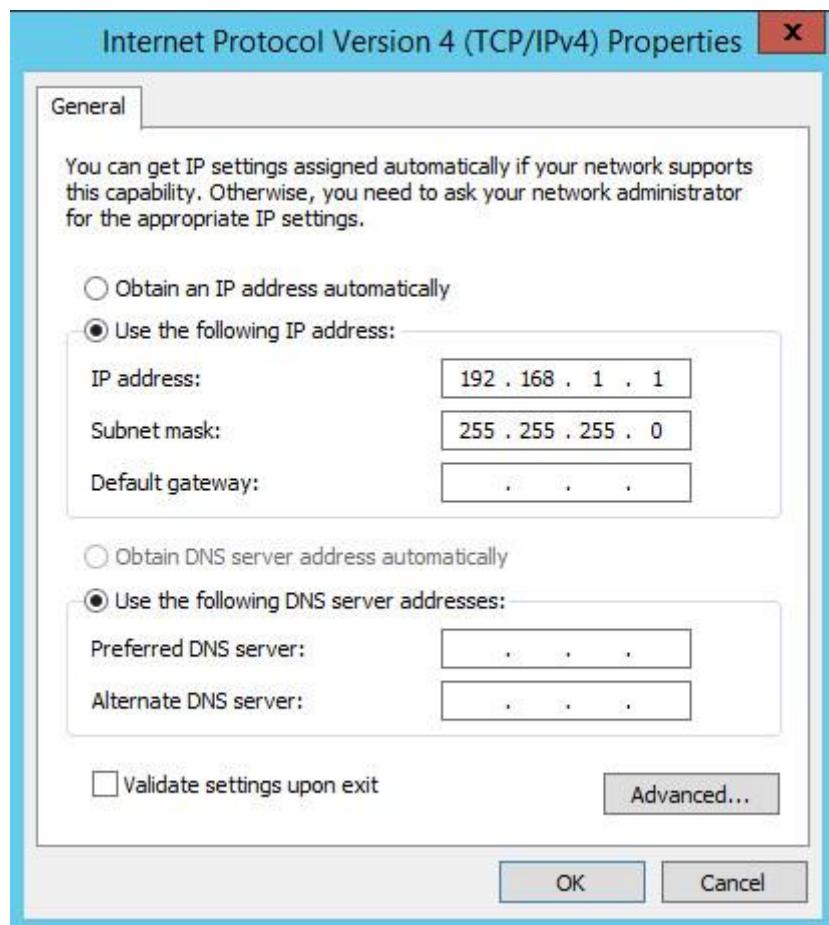


Máy VPN server có 2 card mạng:

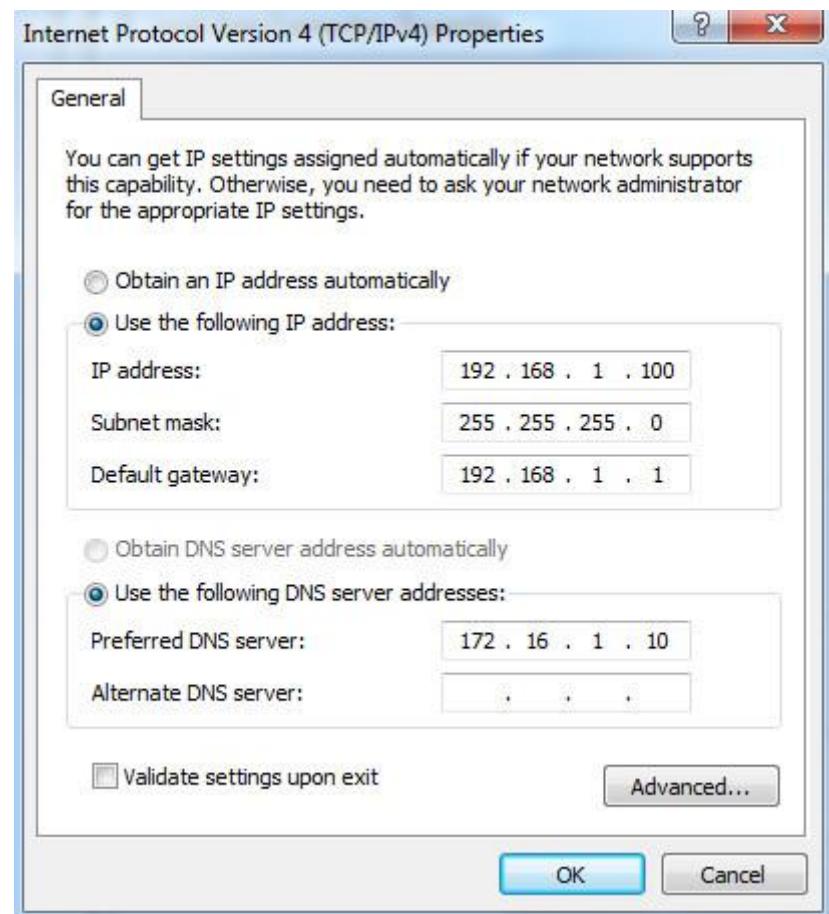
- + Card Internal ta để ở Vmnet0 (của VMWare) có IP như sau



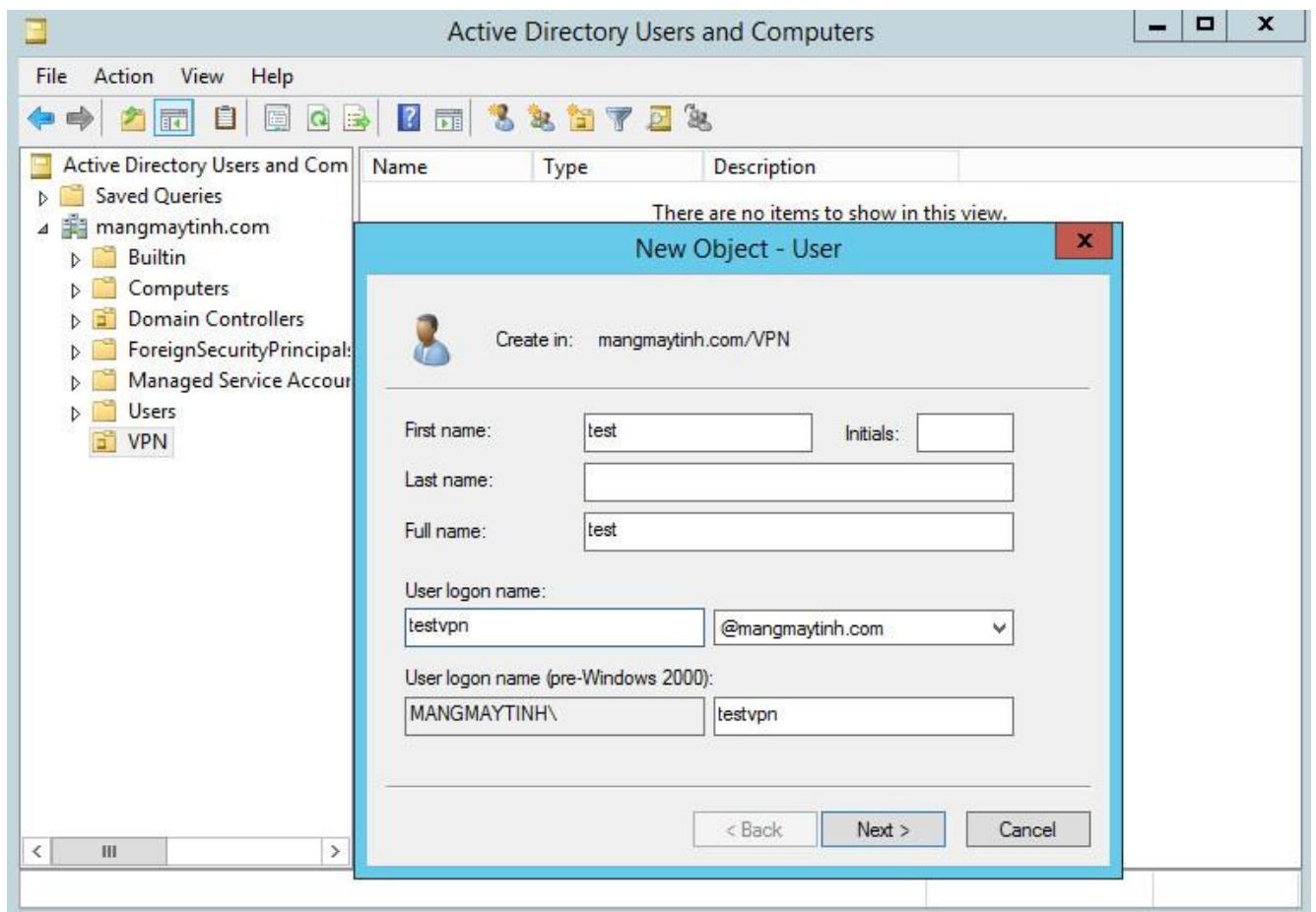
- + Card External ta để Vmnet2 (trong VMWare) có địa chỉ IP như sau



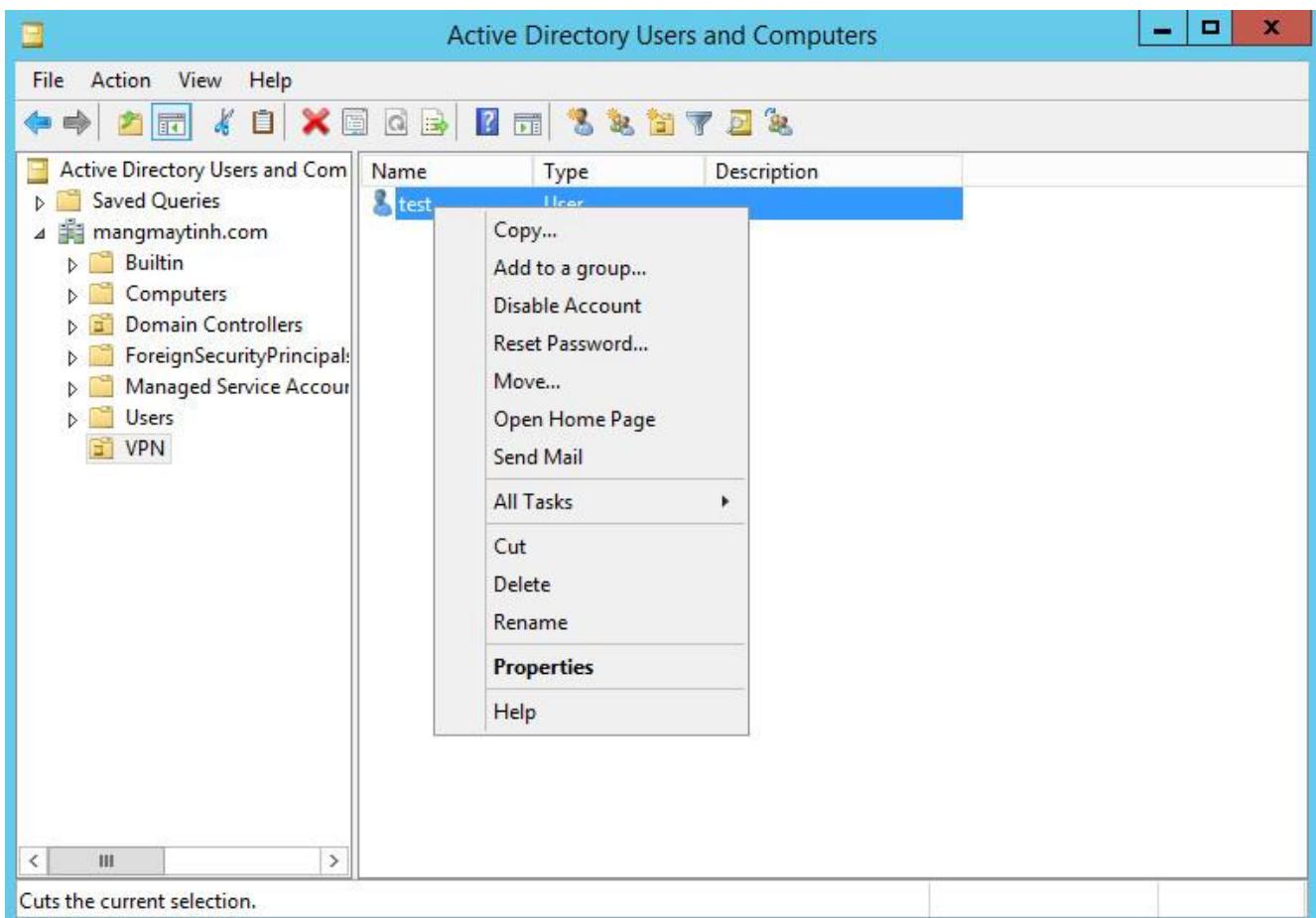
Máy client VPN card mạng ta đê ở Vmnet2 (của VMWare) có IP như sau



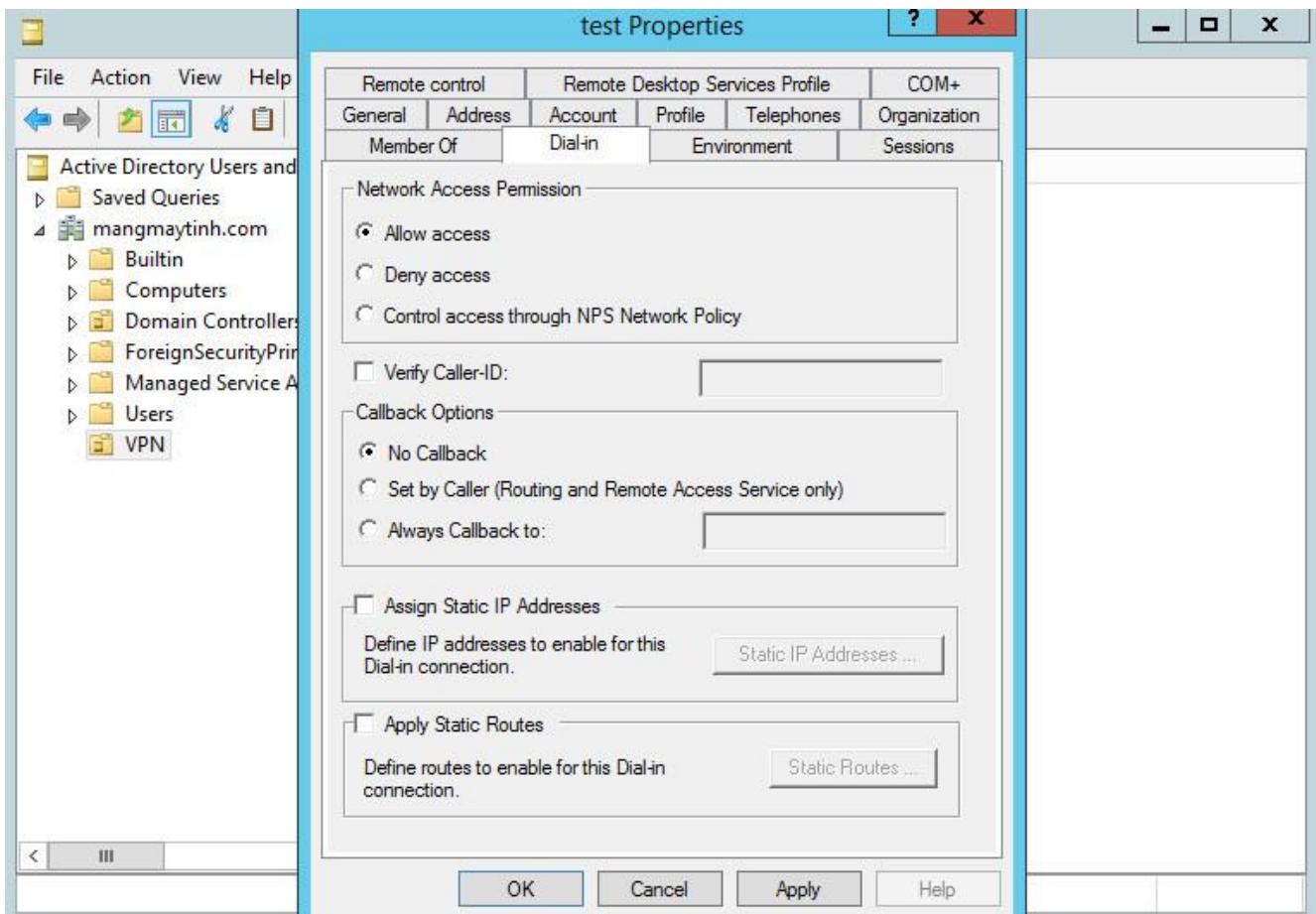
Bước 2: Trên máy DC tạo user và cấp quyền VPN cho user đó



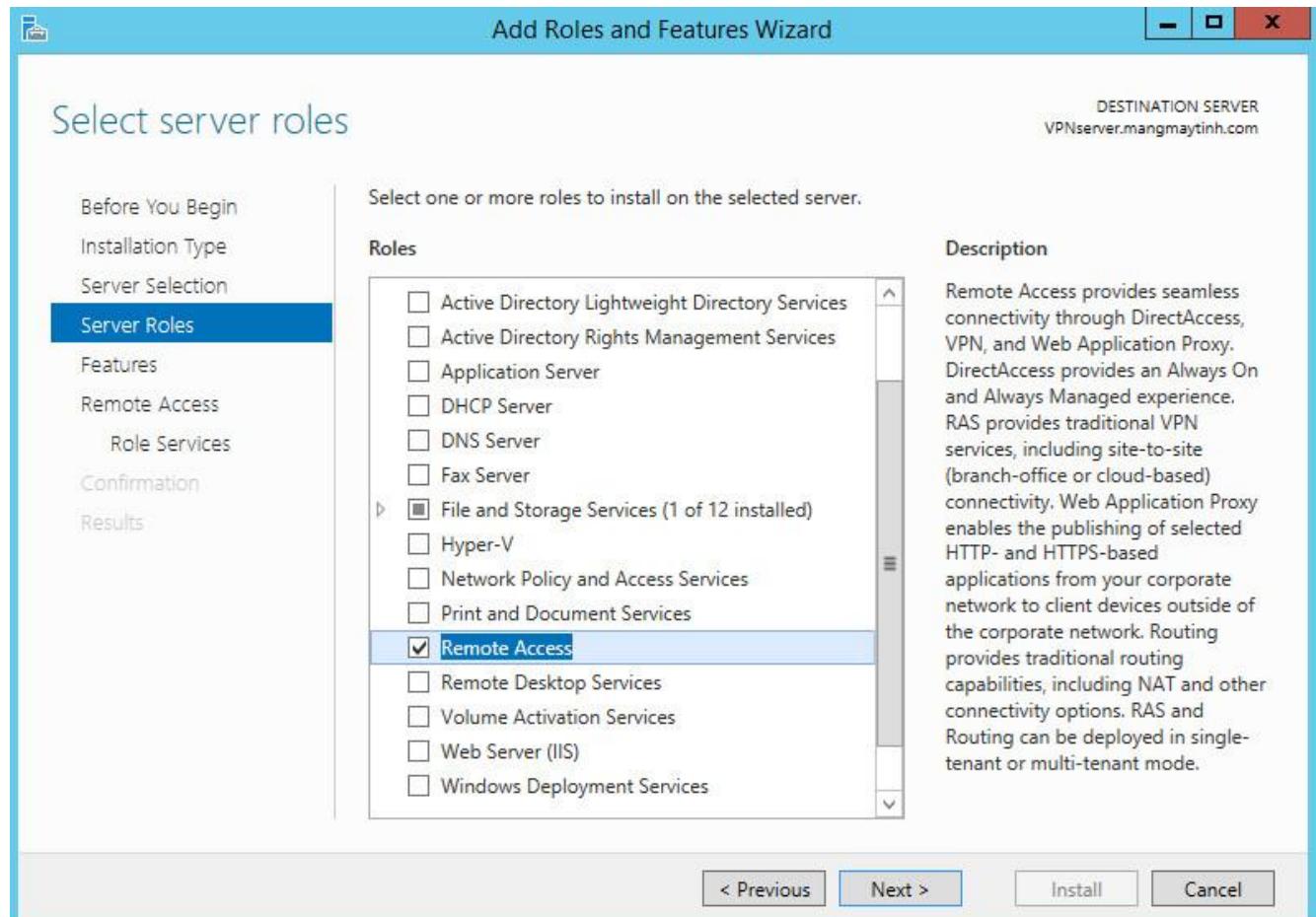
Chuột phải vào user vừa tạo chọn properties



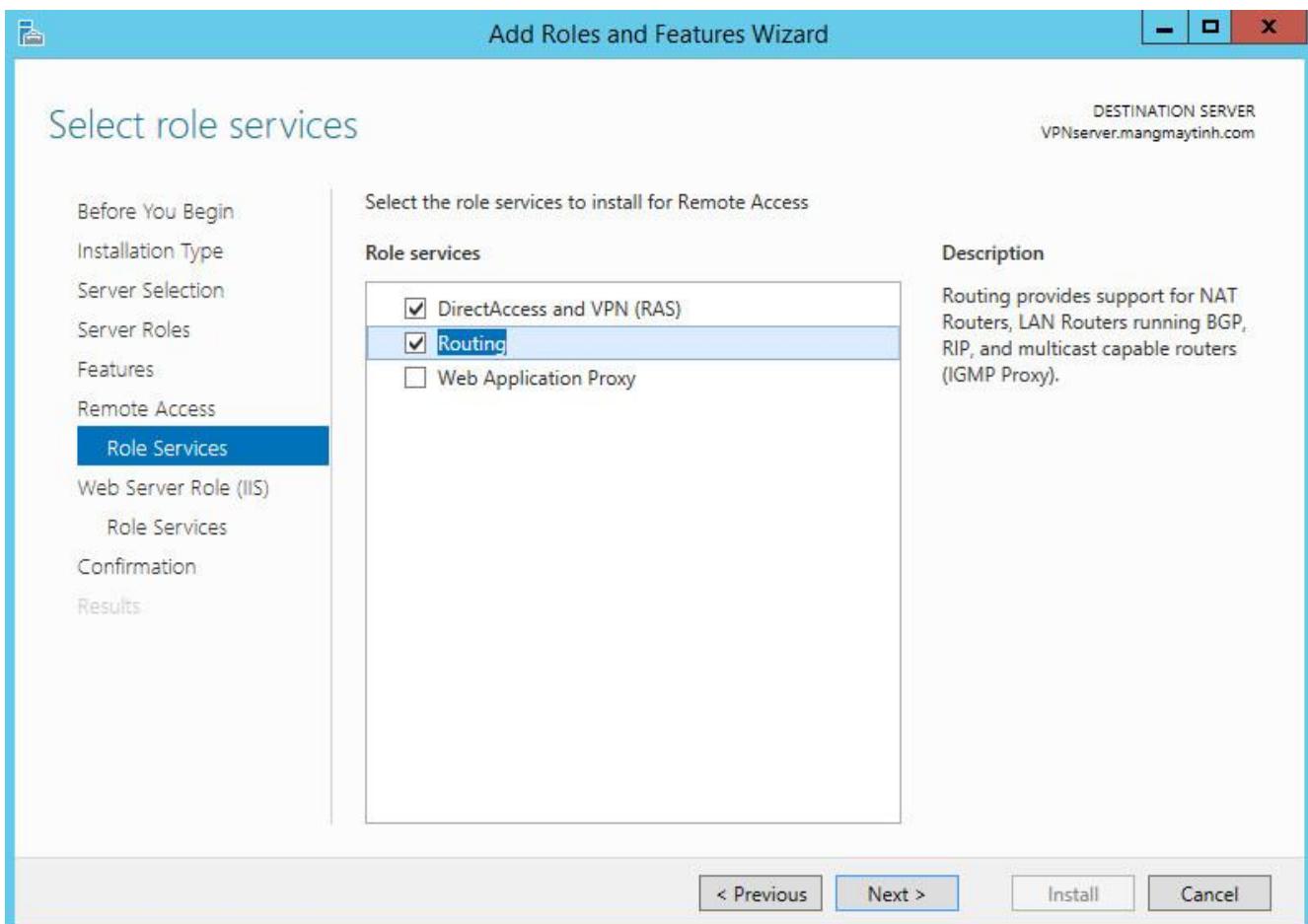
Chọn thẻ Dial-in và kick chọn Allow Access rồi chọn Ok



Bước 3: trên máy VPN server cài đặt Remote Access và cấu hình

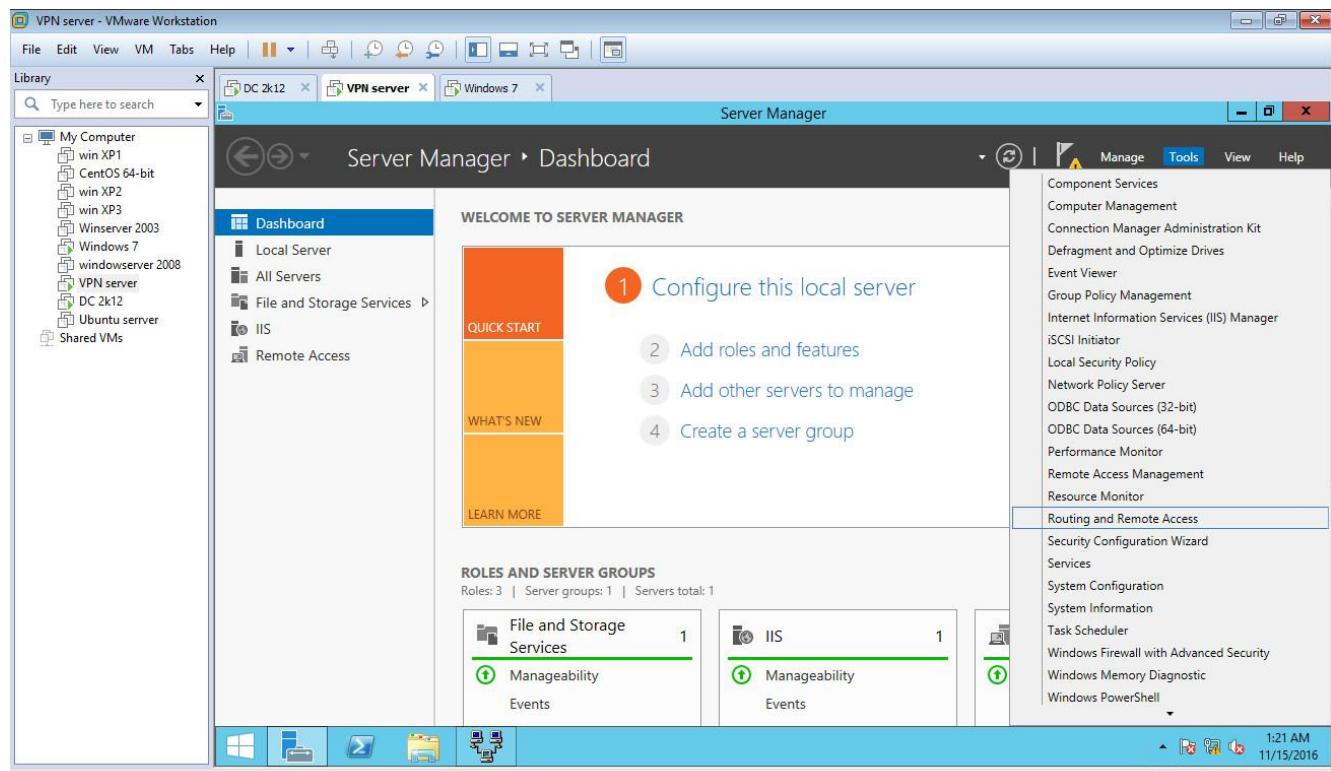


Kick chọn DirectAccess and VPN (RSA) và chọn Routing



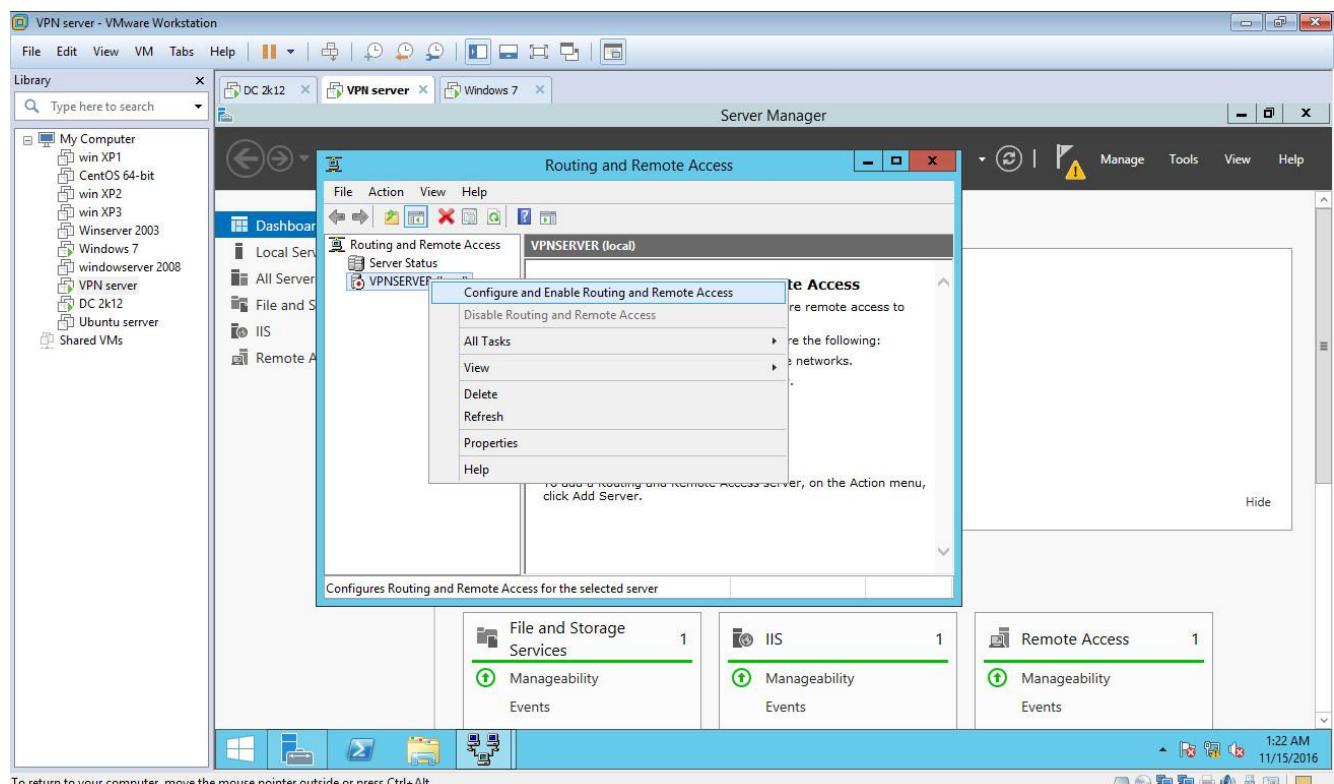
Tiếp tục next cho đến hết

Tiếp theo ta vào Tools chọn Routing and Remote Access

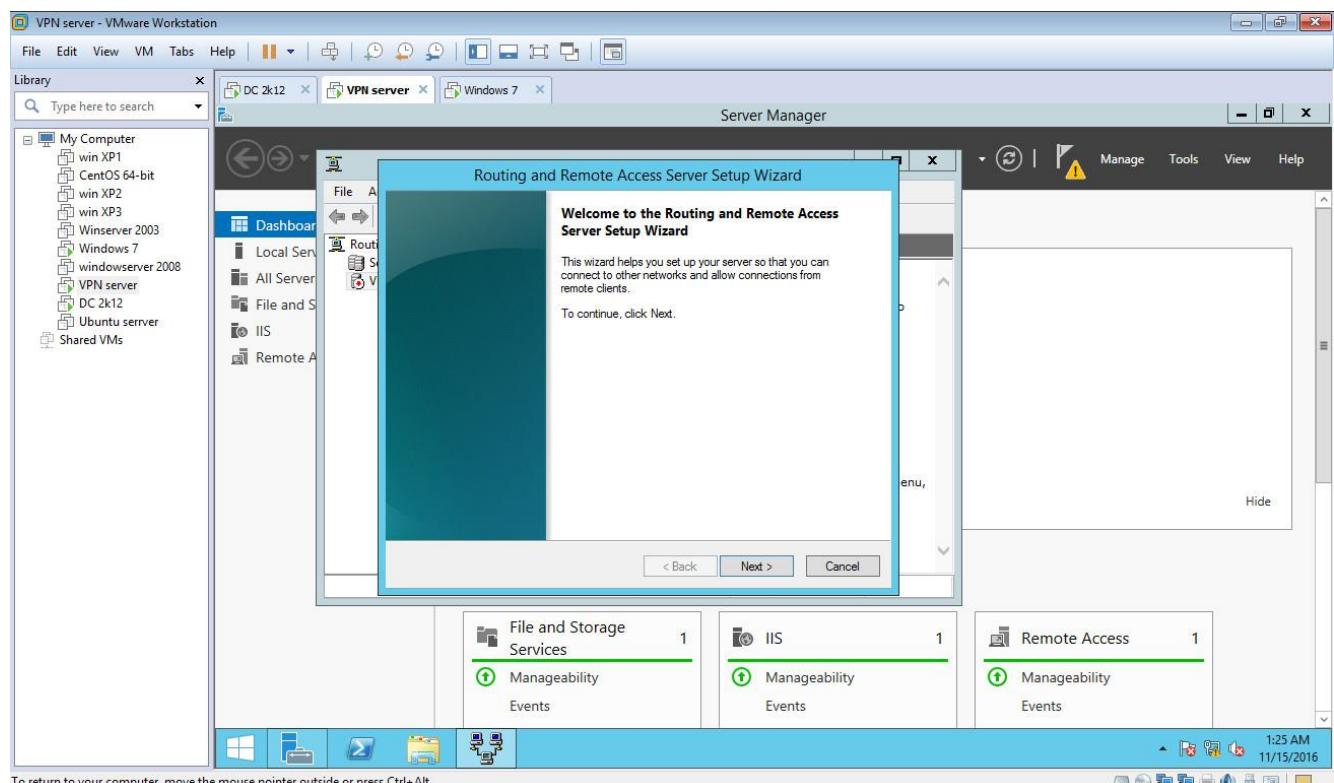


To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

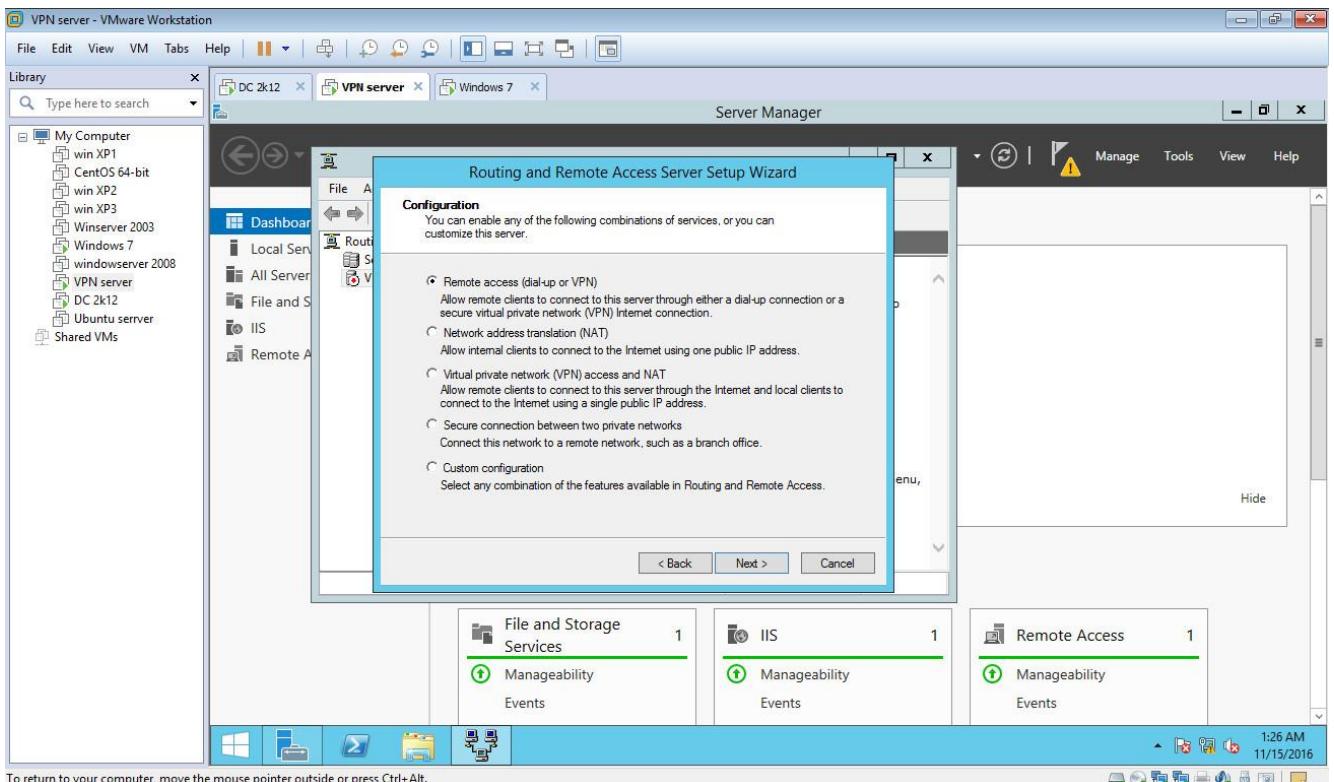
Hộp thoại Routing and Remote Access hiện ra ta ta kick chuột phải vào VPNSERVER và chọn Configure and Enable Routing and Remote Access



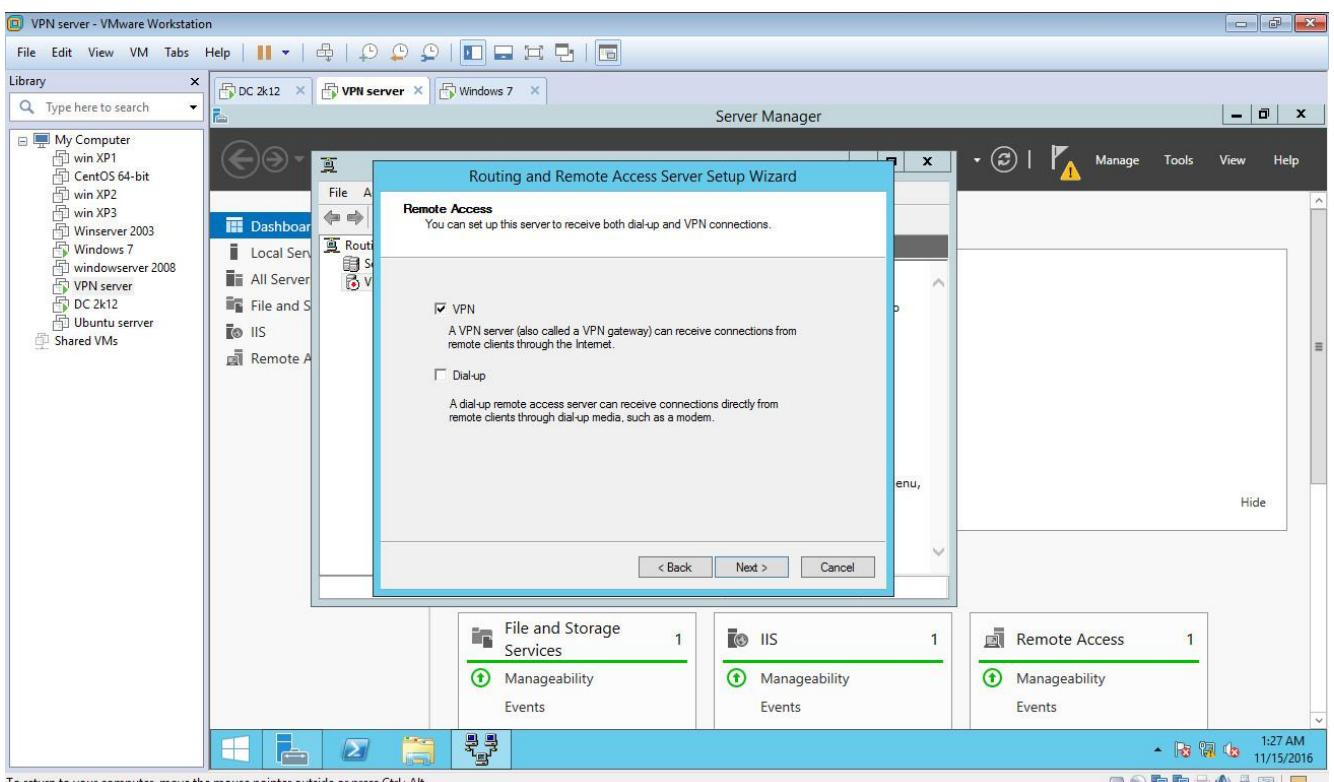
Ta chọn Next



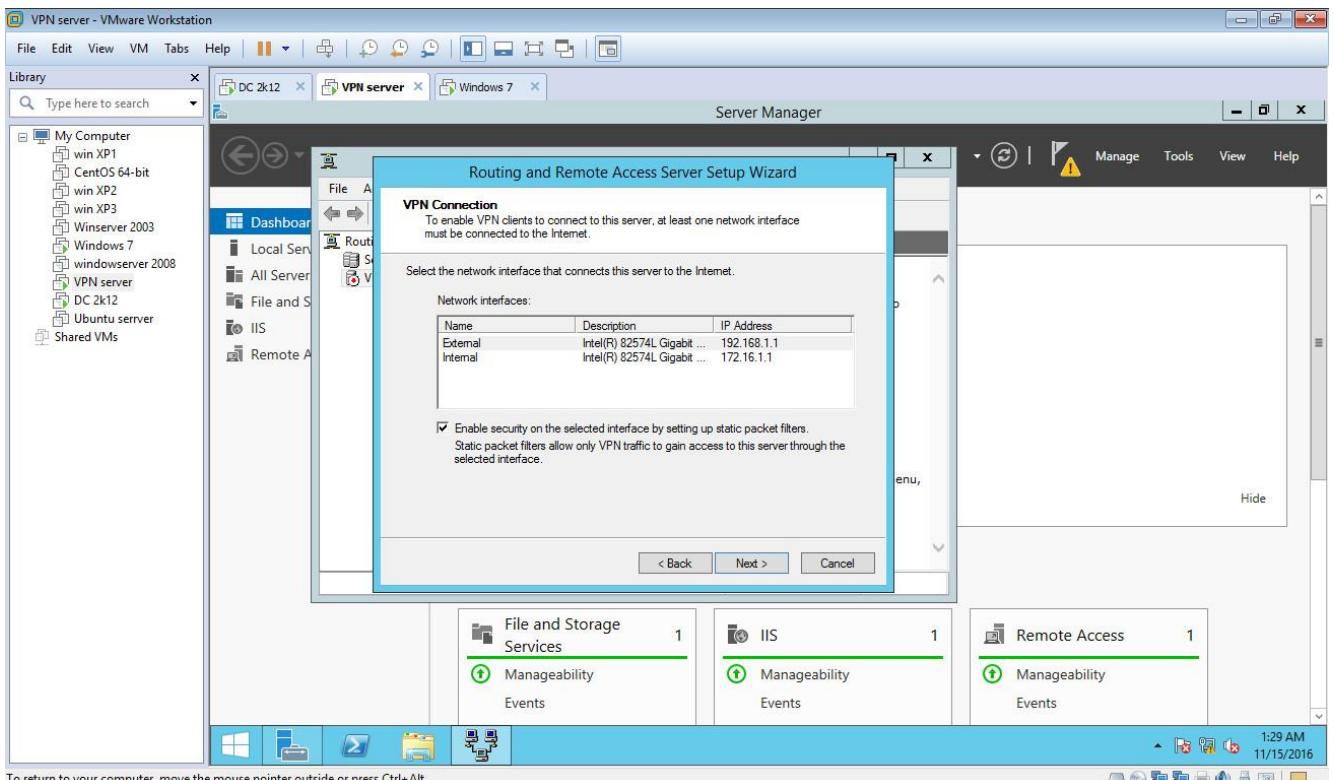
Kick chọn Remote Access rồi kick next



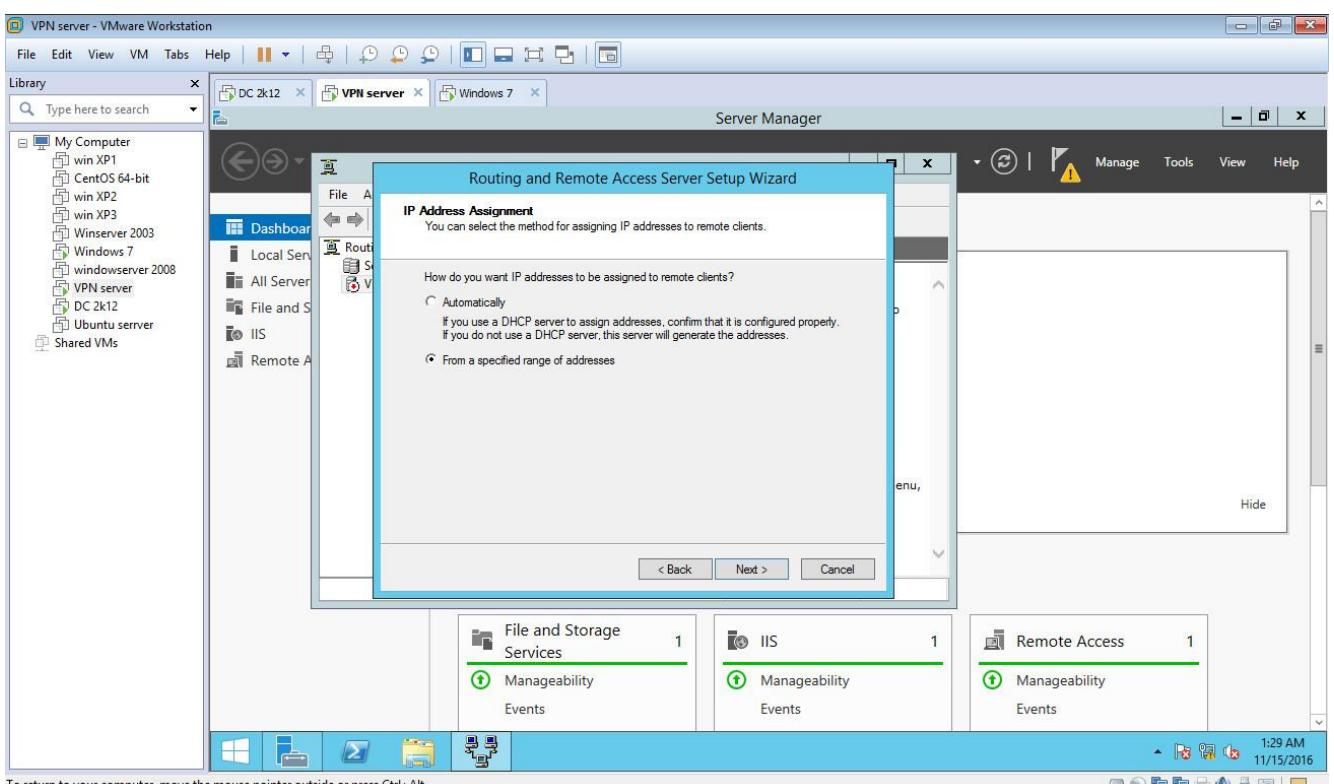
Chọn VPN rồi click next



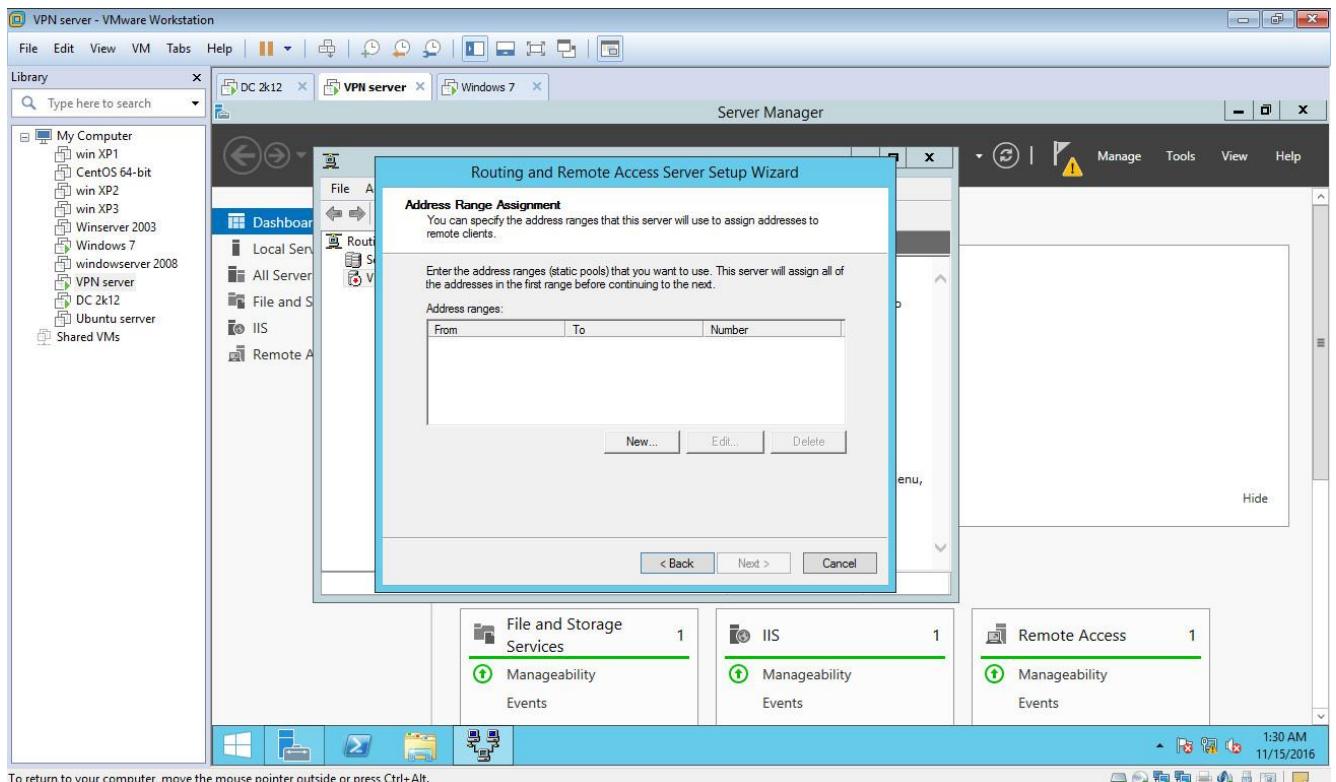
Trên cửa sổ VPN Connection tick chọn card Ext, đây là card bên ngoài của máy VPN Server. Sau đó chọn Next



Trên cửa sổ IP Address Assignment tick chọn From a specified of addresses sau đó chọn Next

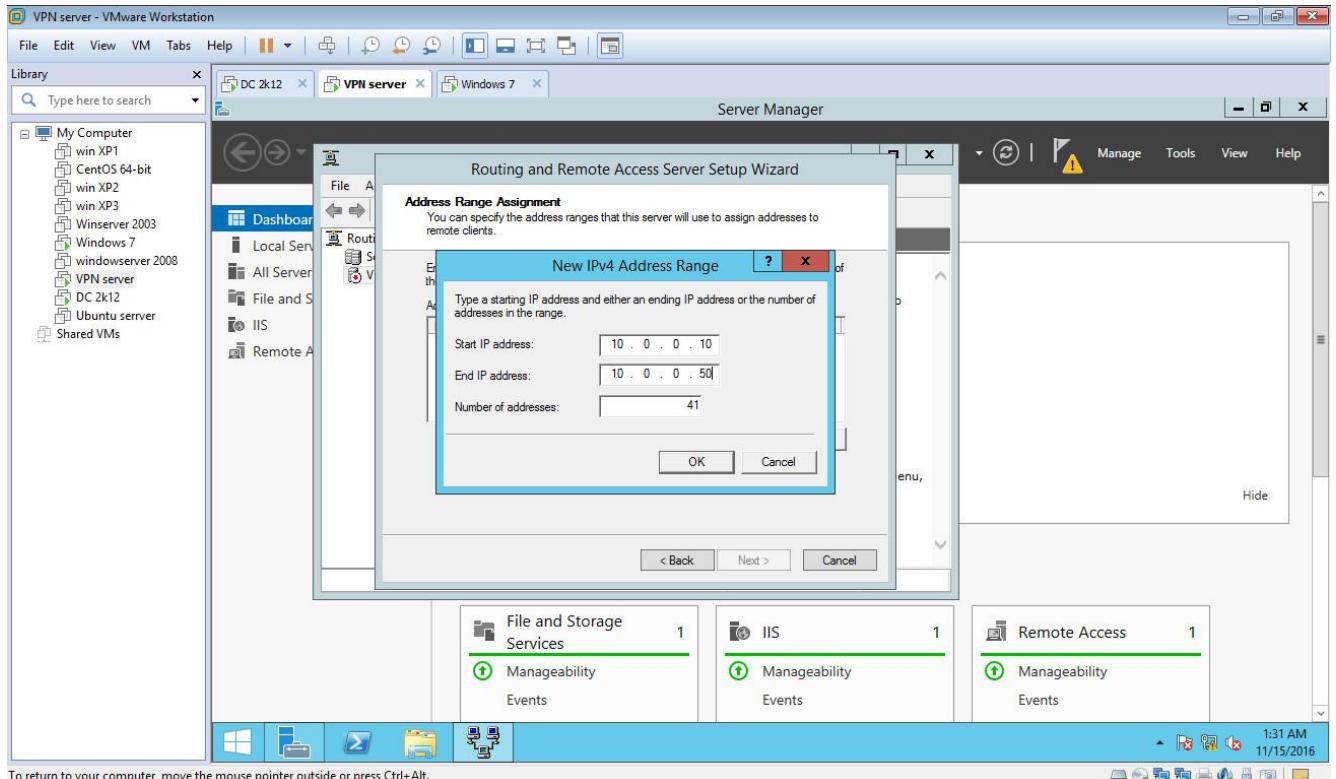


Click New trên cửa sổ Address Range Assignment



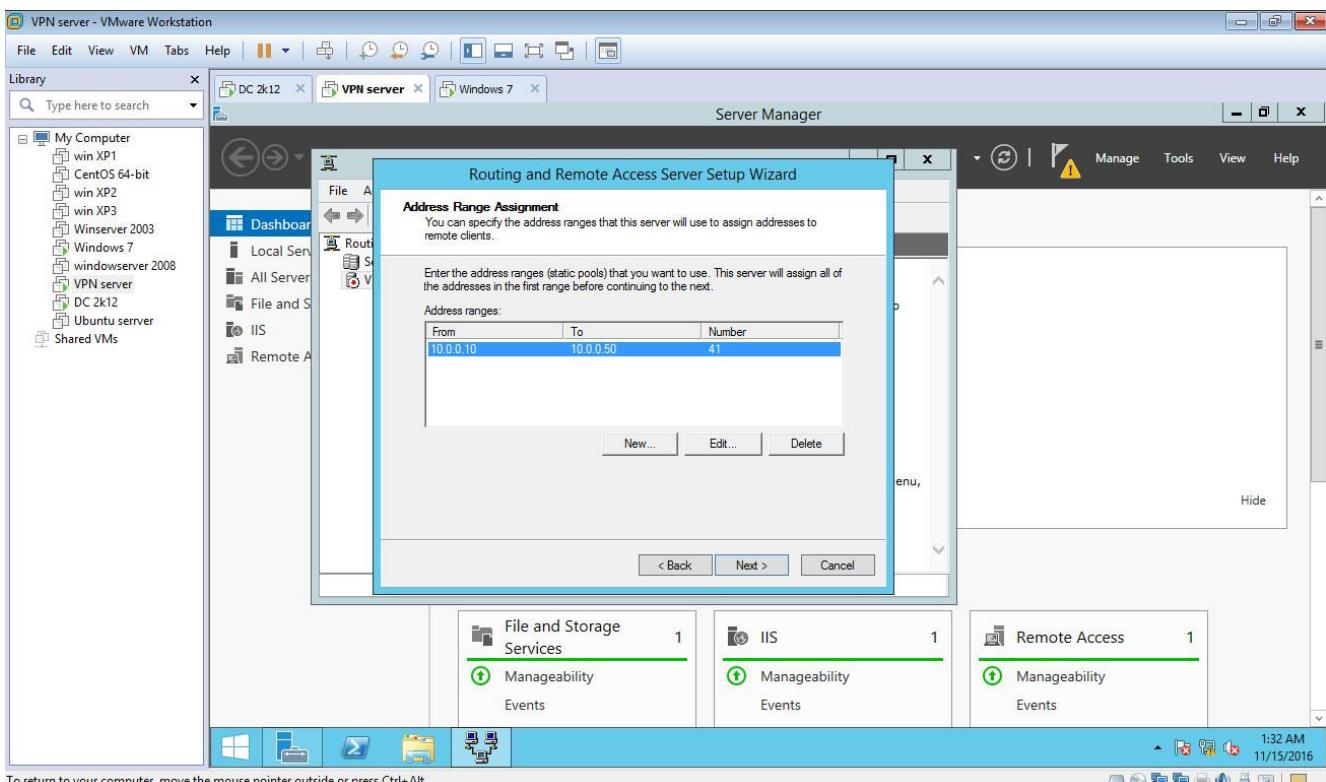
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Gán giải địa chỉ IP mà các máy Client sẽ nhận. Có thể gán bất kì 1 giải nào sau đó chọn OK

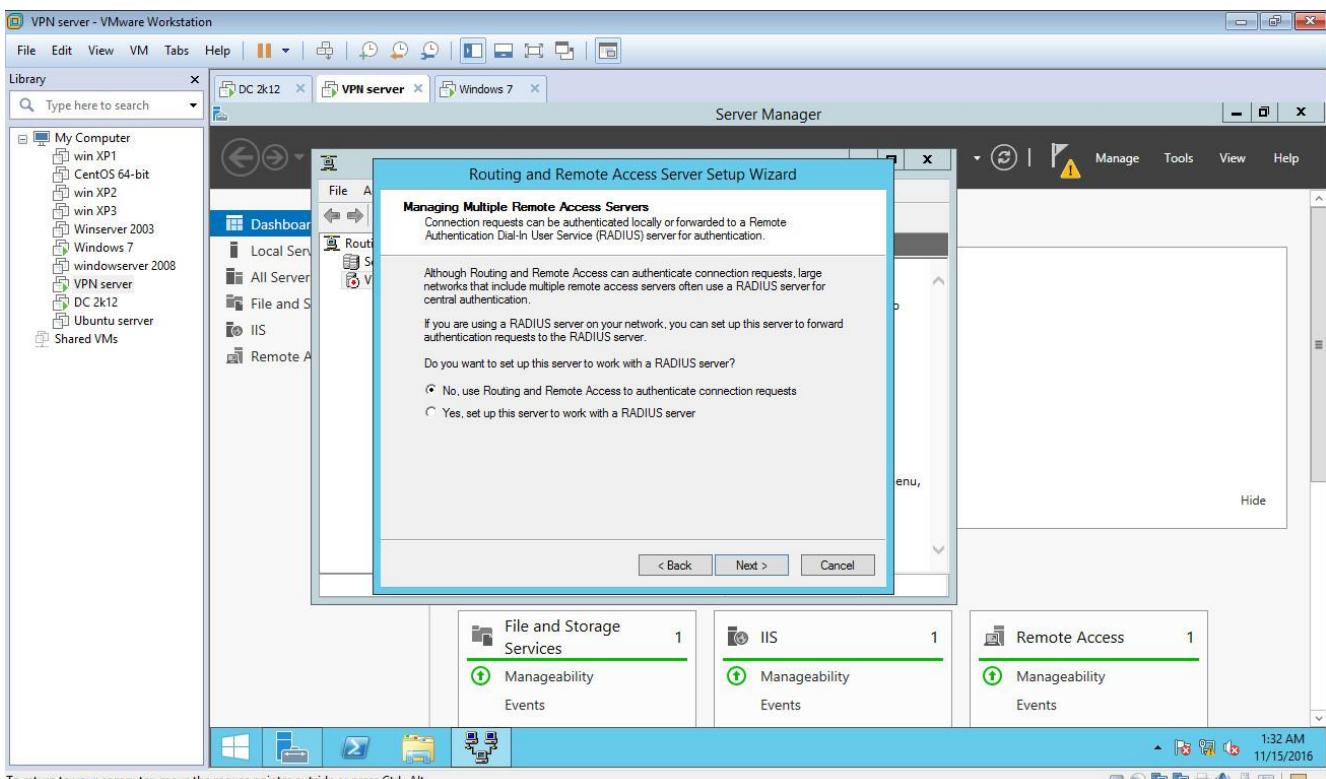


To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

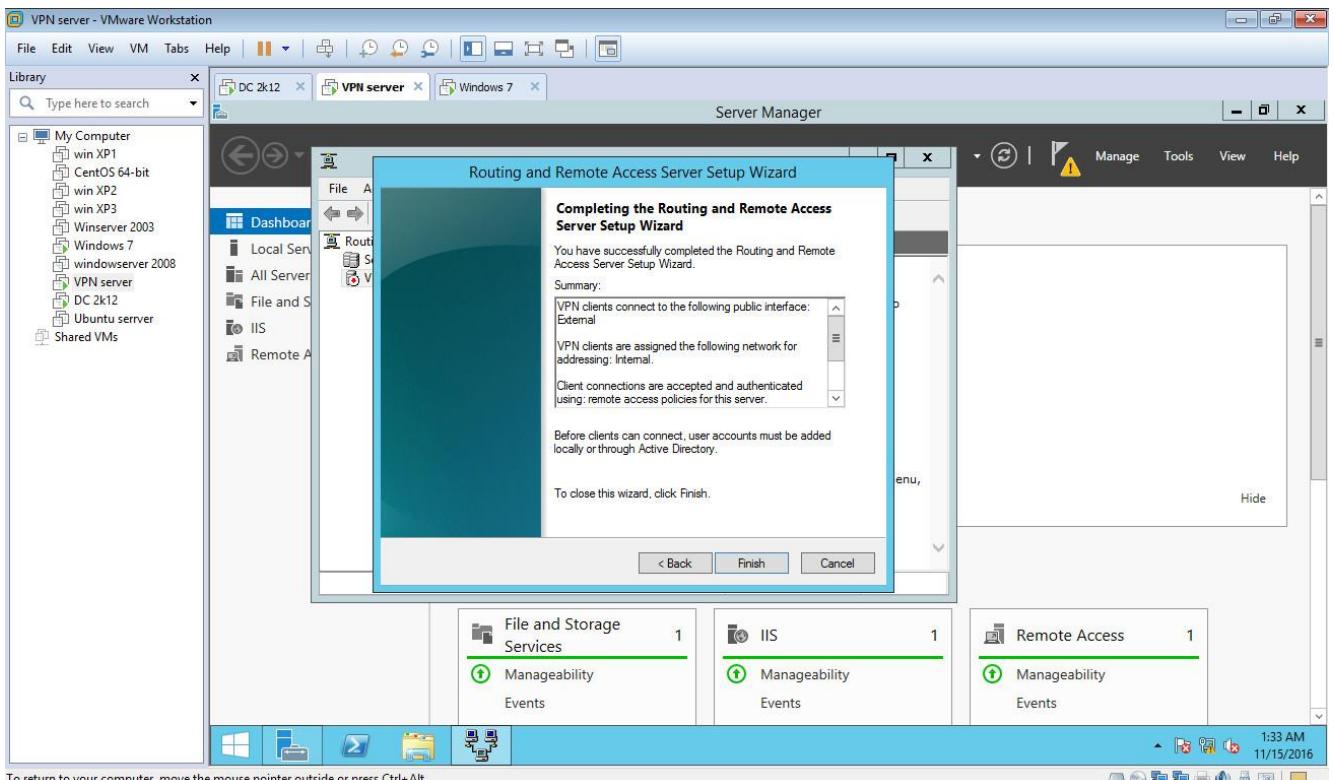
Click Next trên cửa sổ Address Range Assignment



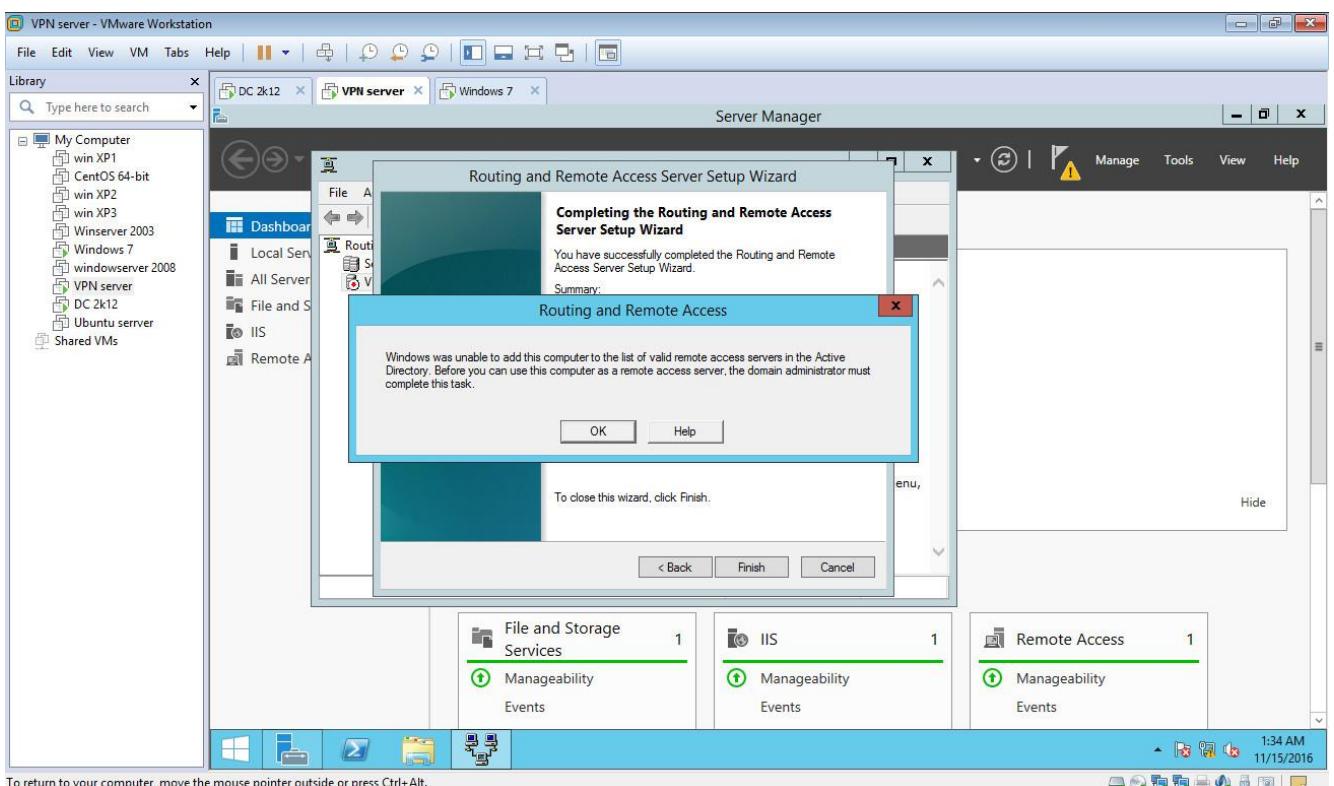
Tích chọn No, Use Routing and Remote Access to authenticate connection requests và sau đó chọn Next



Click Finish để kết thúc quá trình cấu hình

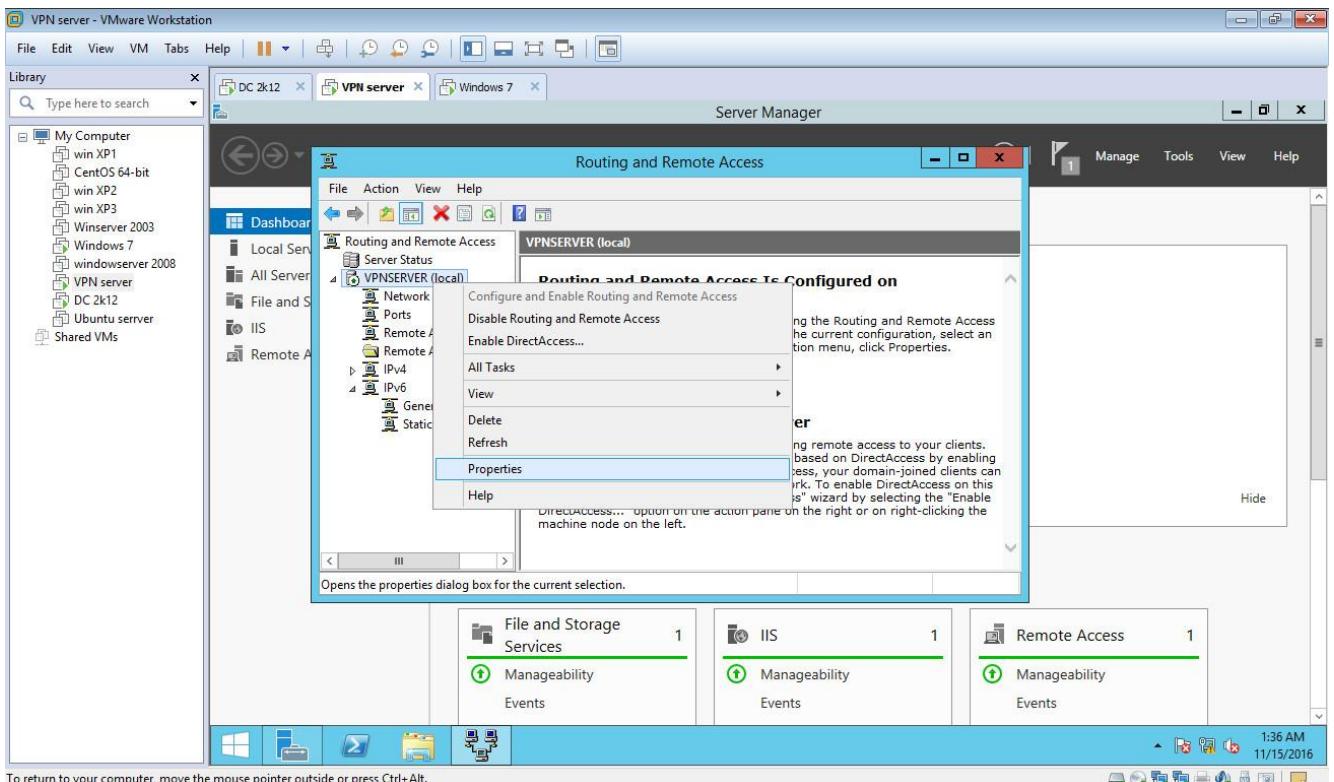


Click OK để khởi động dịch vụ RRAS

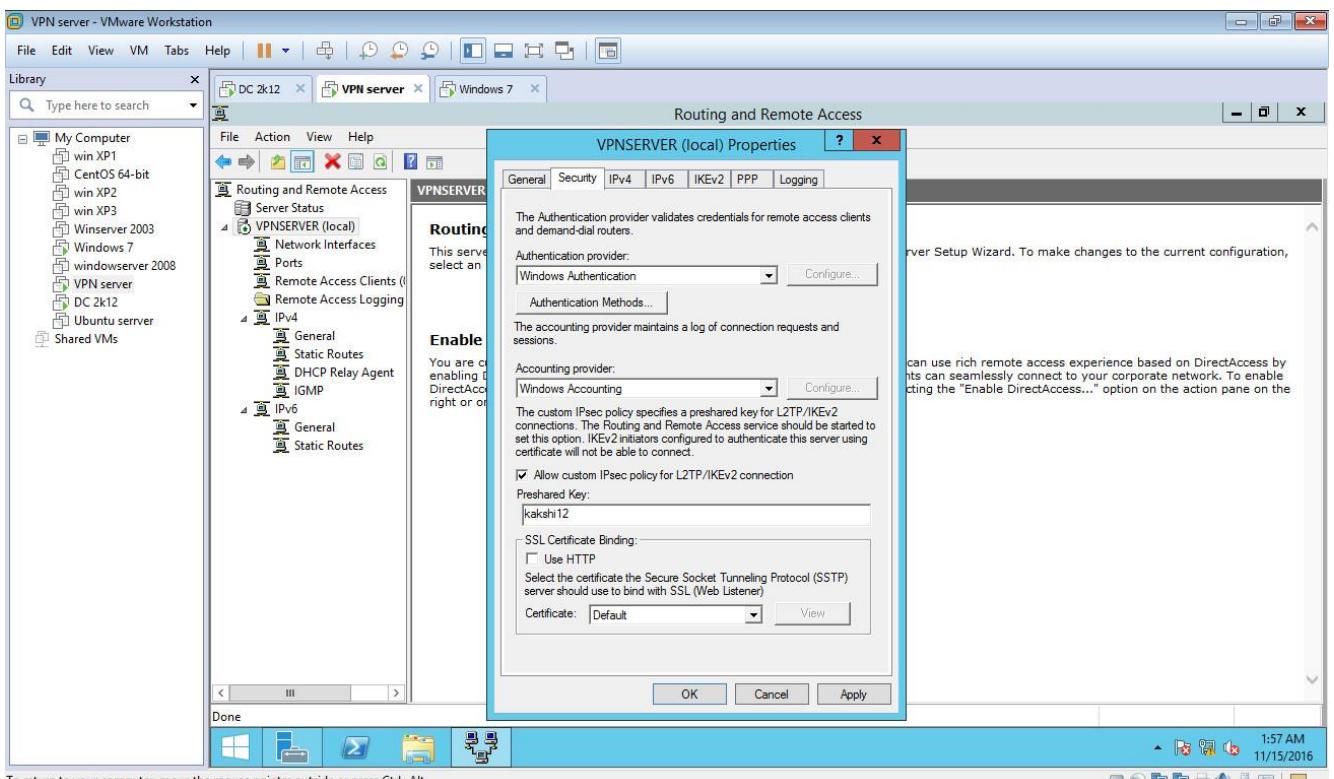


Bước 4: Cấu hình tạo key và sử dụng giao thức L2TP

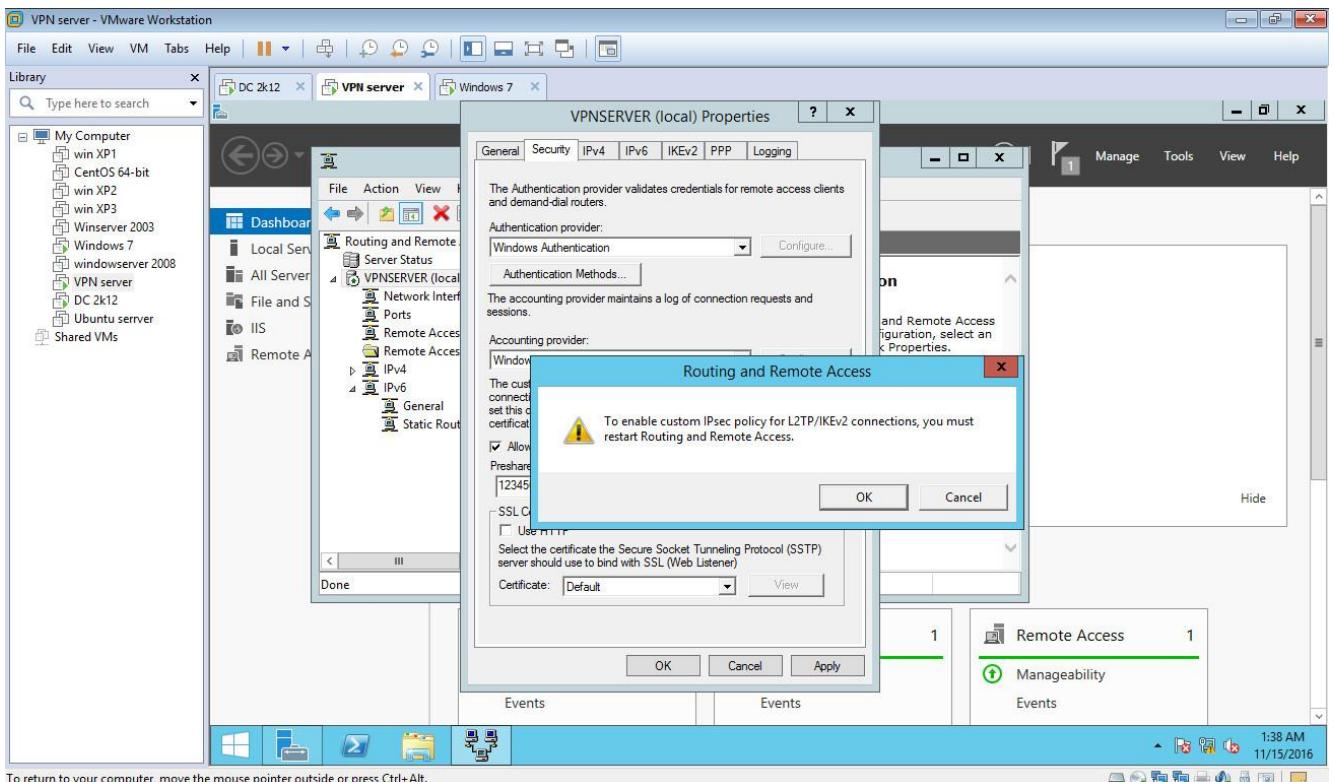
Vào Administrative tool —> Routing and Remote Access. Click chuột phải vào Vpnserver (local) chọn Properties



Trên tab Security, tick chọn Allow custom IPsec policy for L2TP connection, gán Key tùy chọn tại ô Preshared Key. Click OK

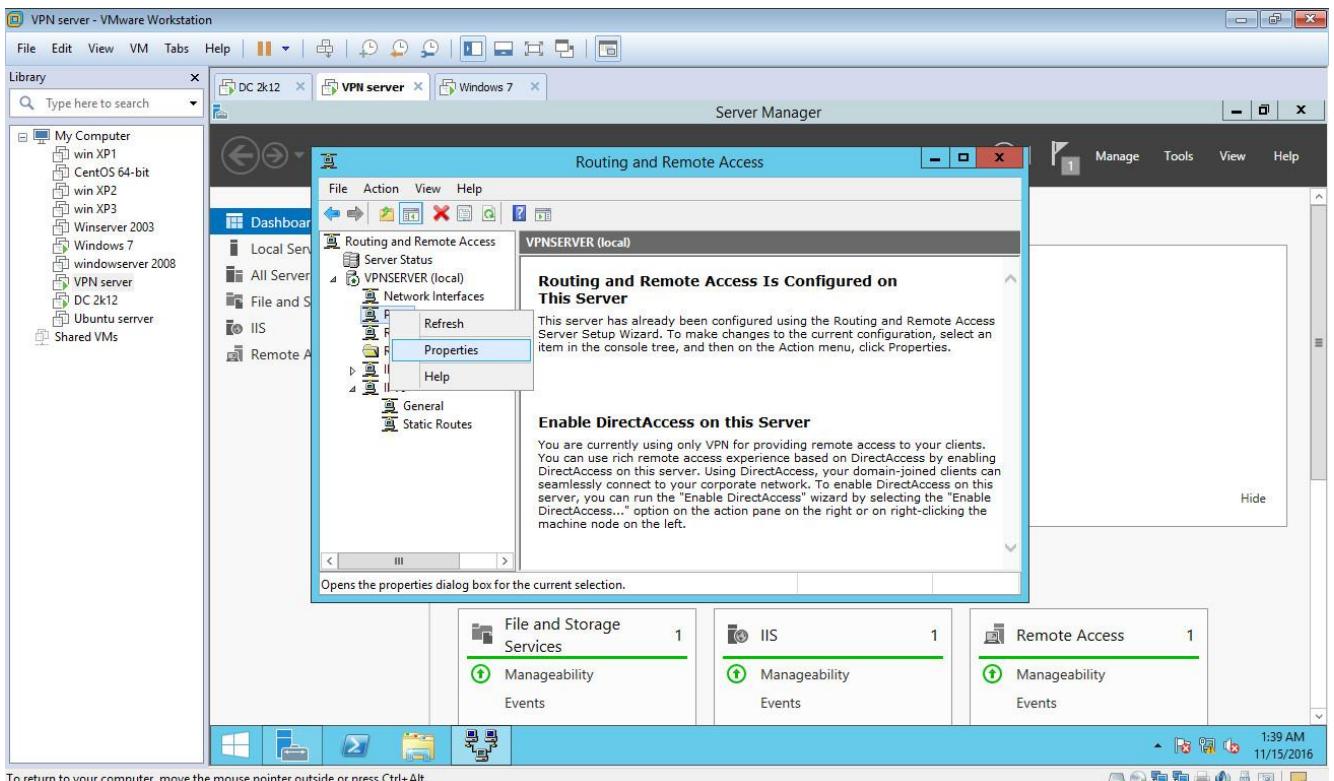


Click OK để xác nhận

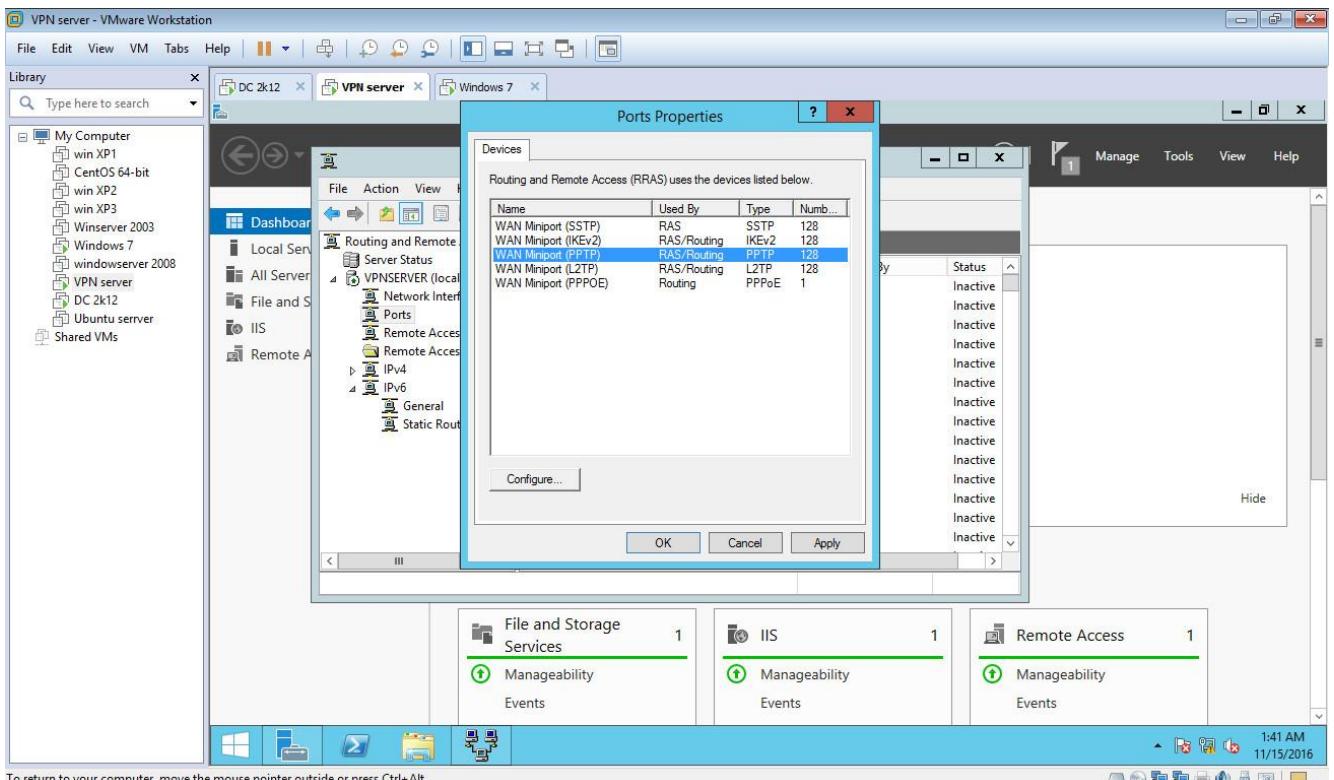


Ngăn VPN Client sử dụng giao thức PPTP và SSTP

Click chuột phải vào Port chọn Properties

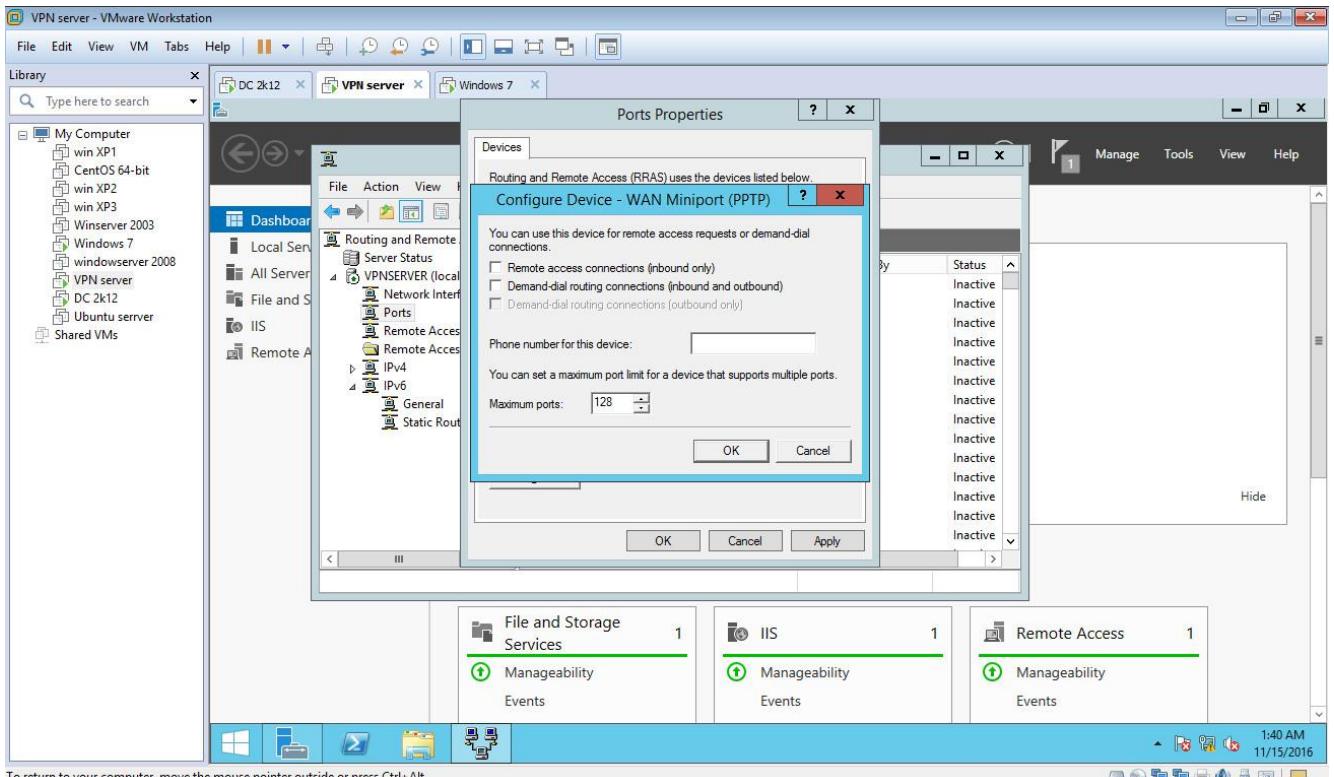


Trên màn hình Ports Properties, click chọn giao thức PPTP sau đó chọn Configure....



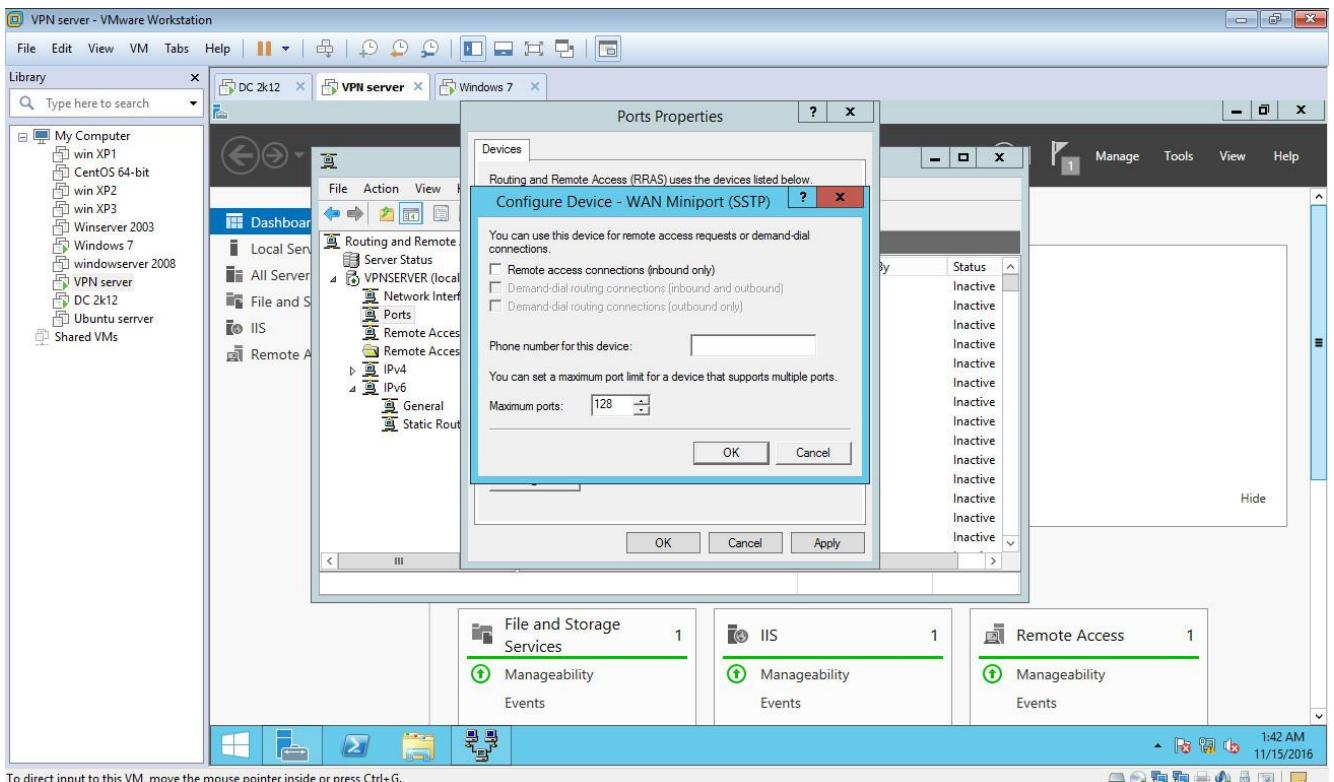
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Bỏ dấu tick tại Remote access connections (inbound only) và Demand-dial routing connections (inbound and outbound)

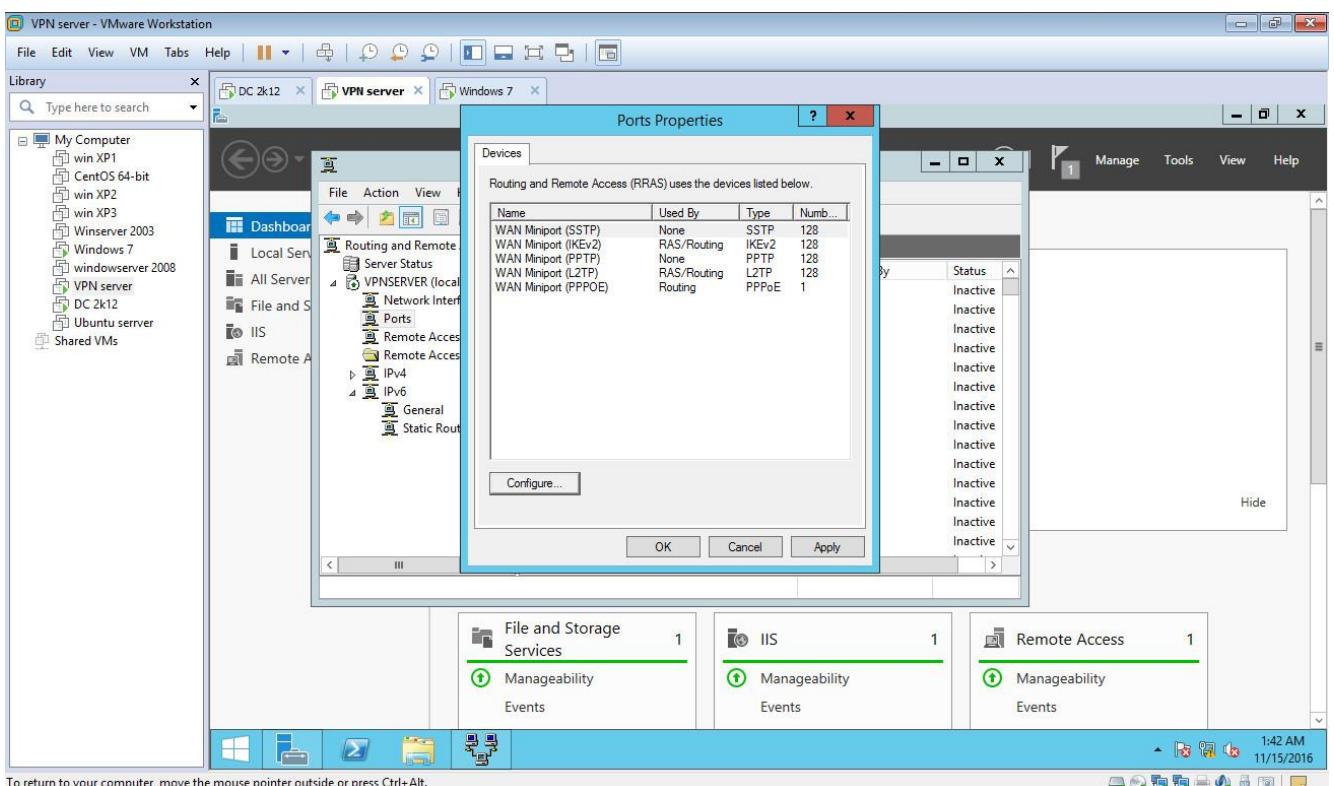


To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

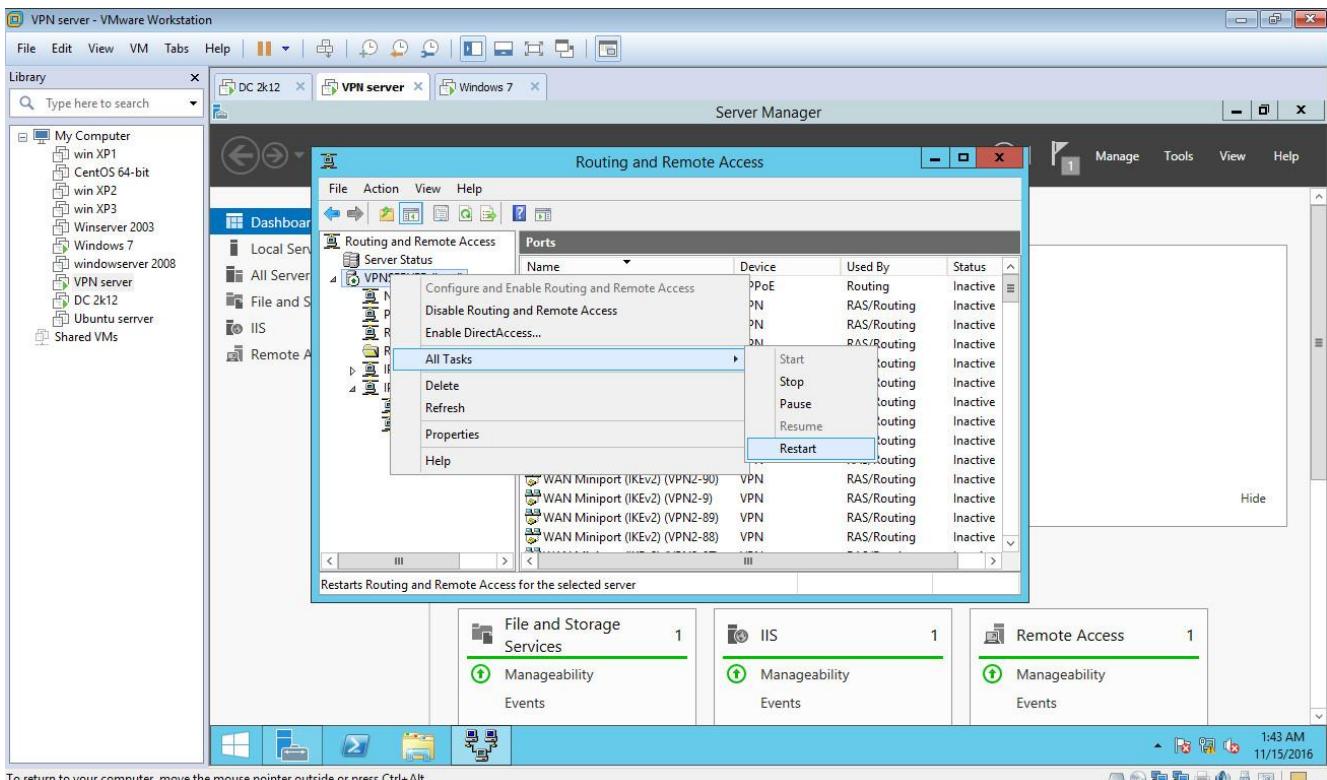
Tương tự với giao thức SSTP, bỏ dấu tick tại Remote access connections (inbound only)



Kết quả như sau



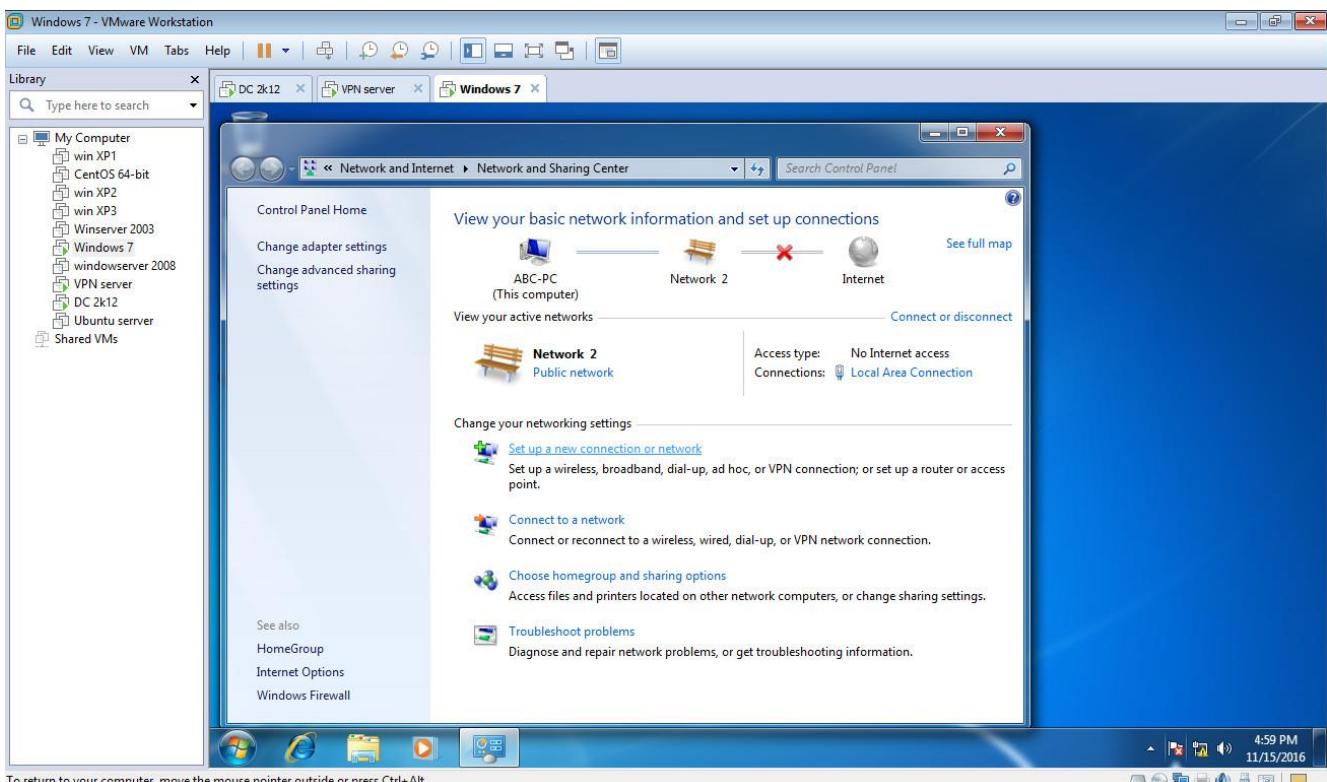
Sau khi cấu hình xong, cần restart lại dịch vụ RRAS



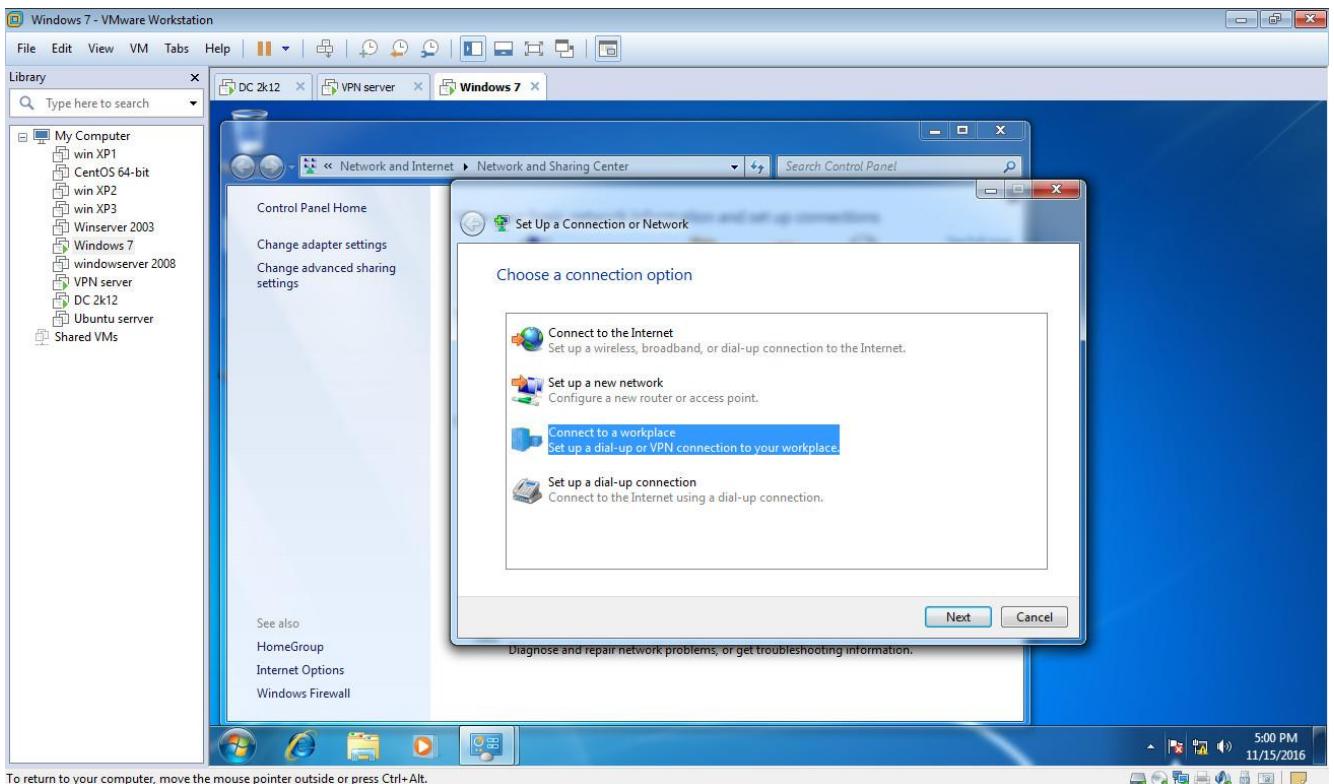
Bước 5: Tạo kết nối VPN và cấu hình VPN bằng giao thức L2TP

Thực hiện trên máy Client1

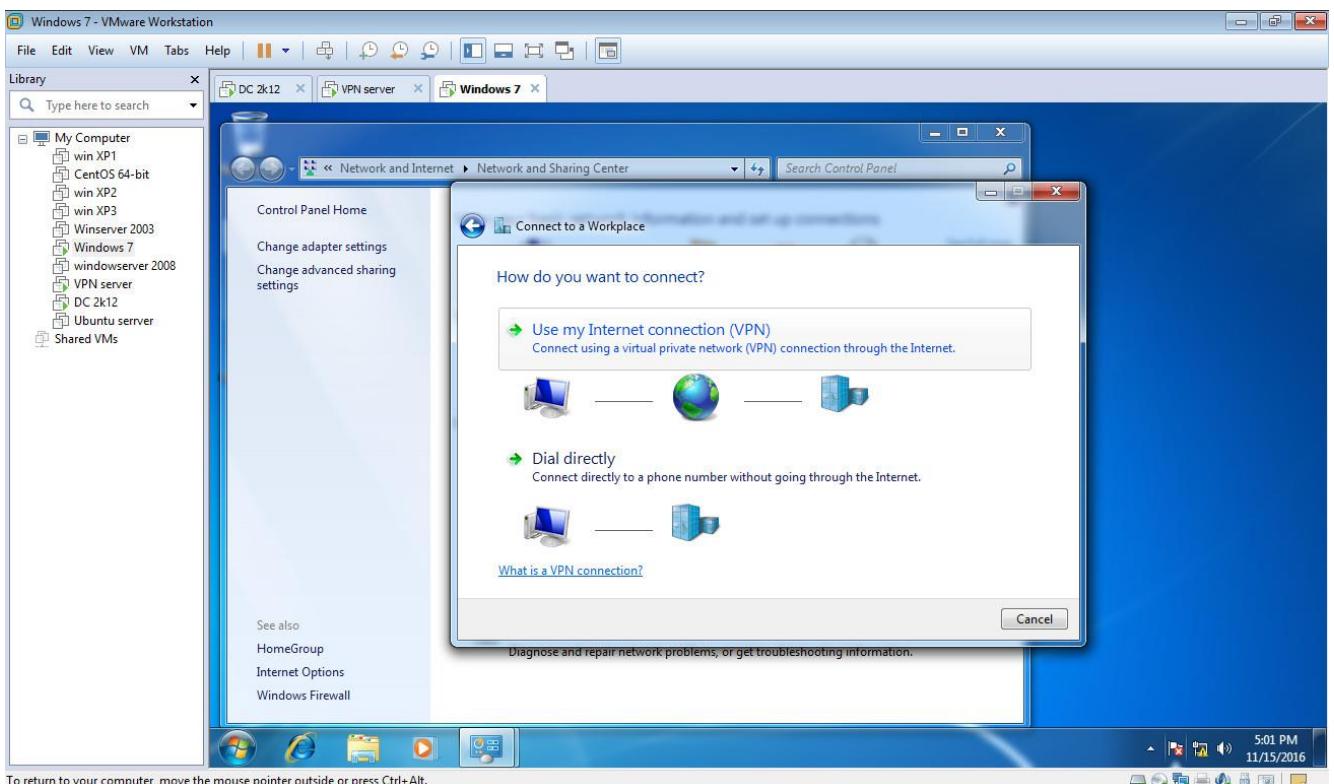
Vào Network and Sharing Center, chọn Set up a new connection or network.



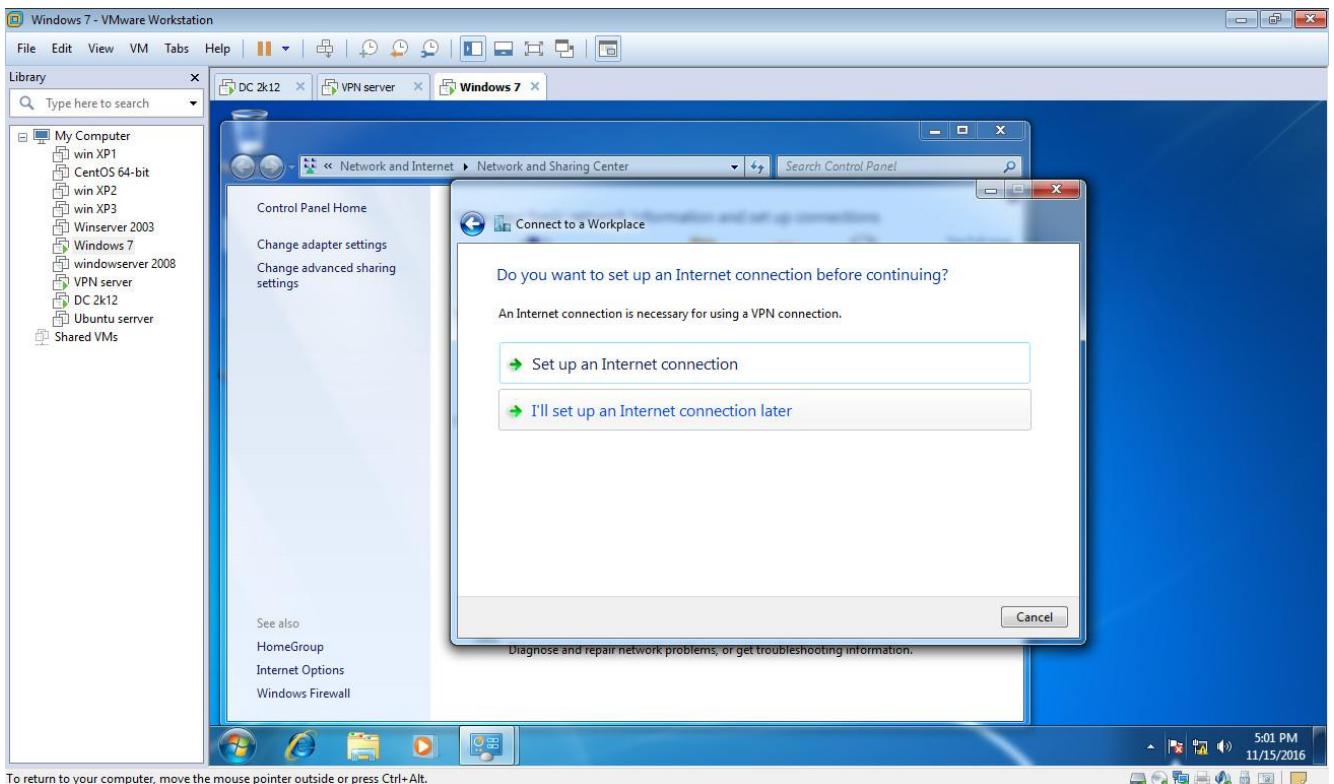
Tick chọn Connect to workplace, sau đó chọn Next



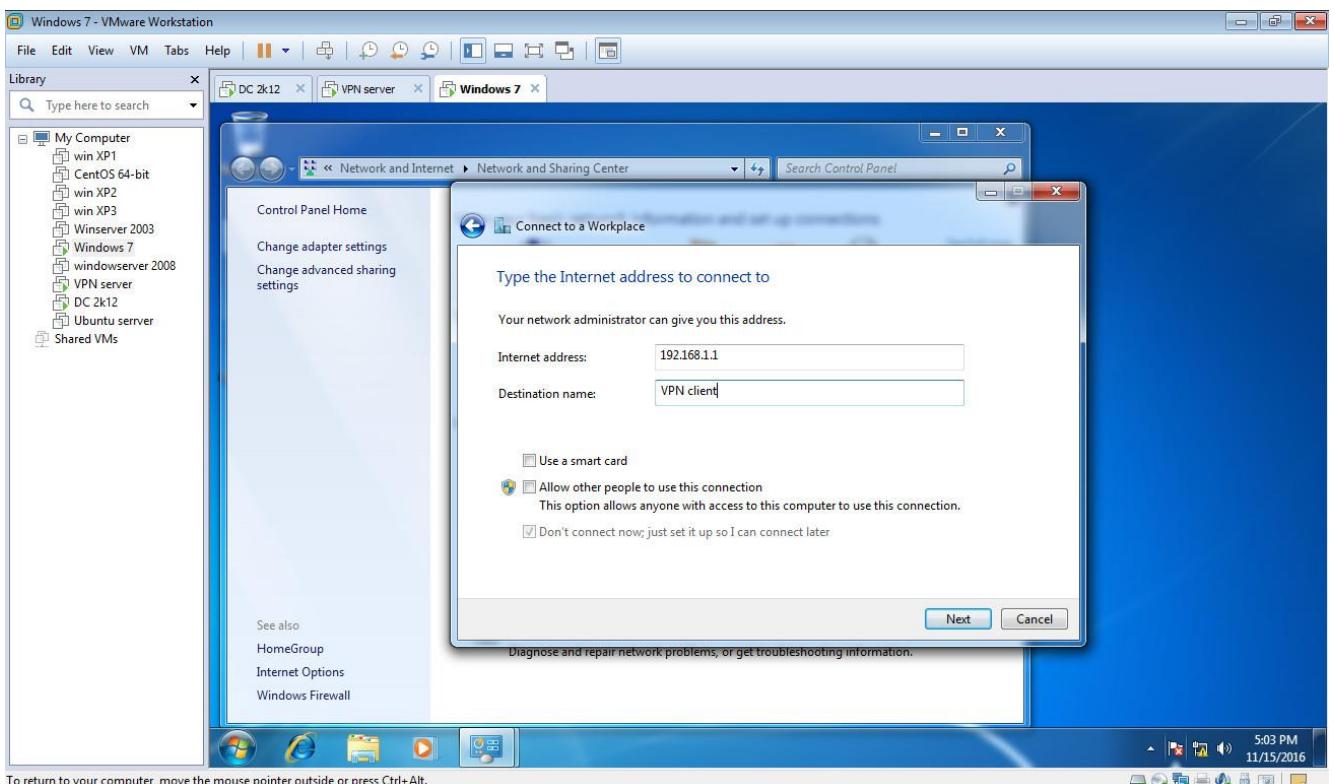
Click chọn Use my internet connection (VPN) và sau đó chọn Next



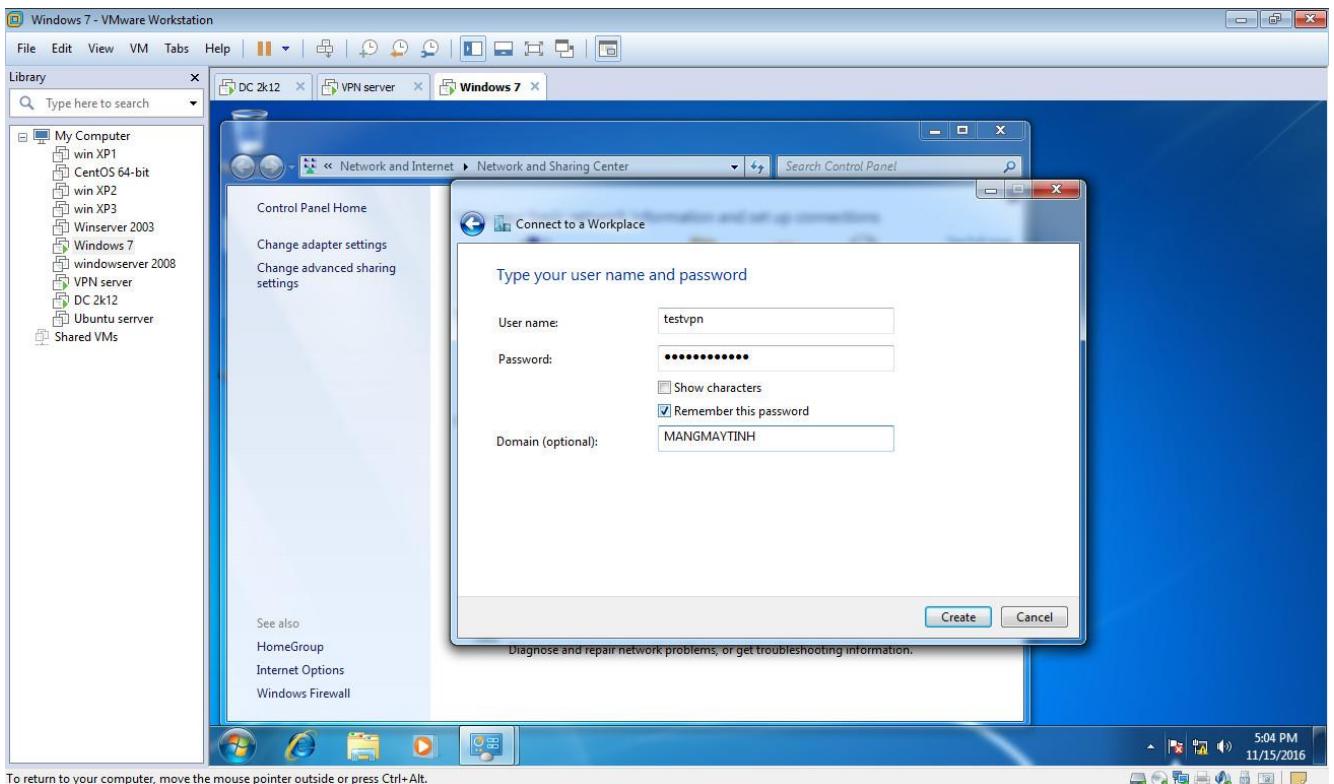
Click chọn I'll set up an Internet connection later sau đó chọn Next



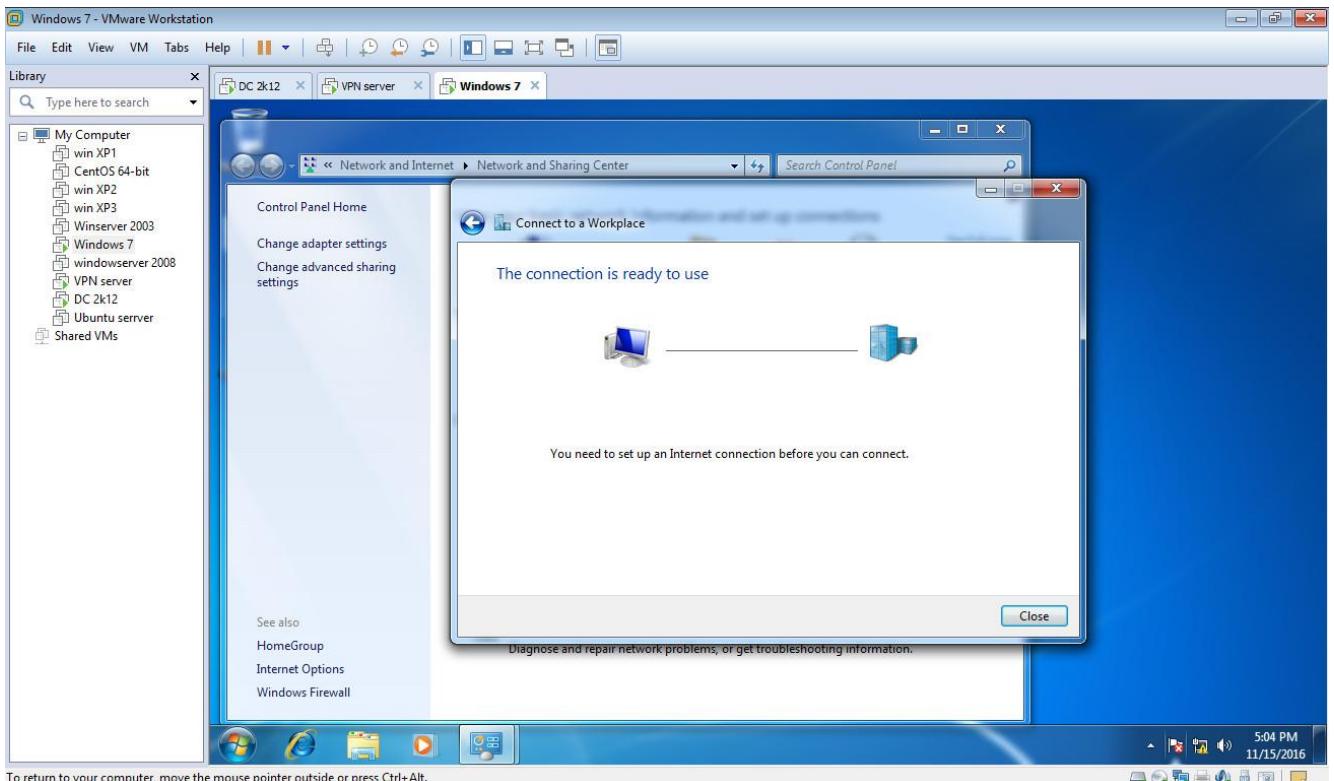
Điền địa chỉ IP public của máy VPN Server là địa chỉ của card Ext sau đó chọn Next



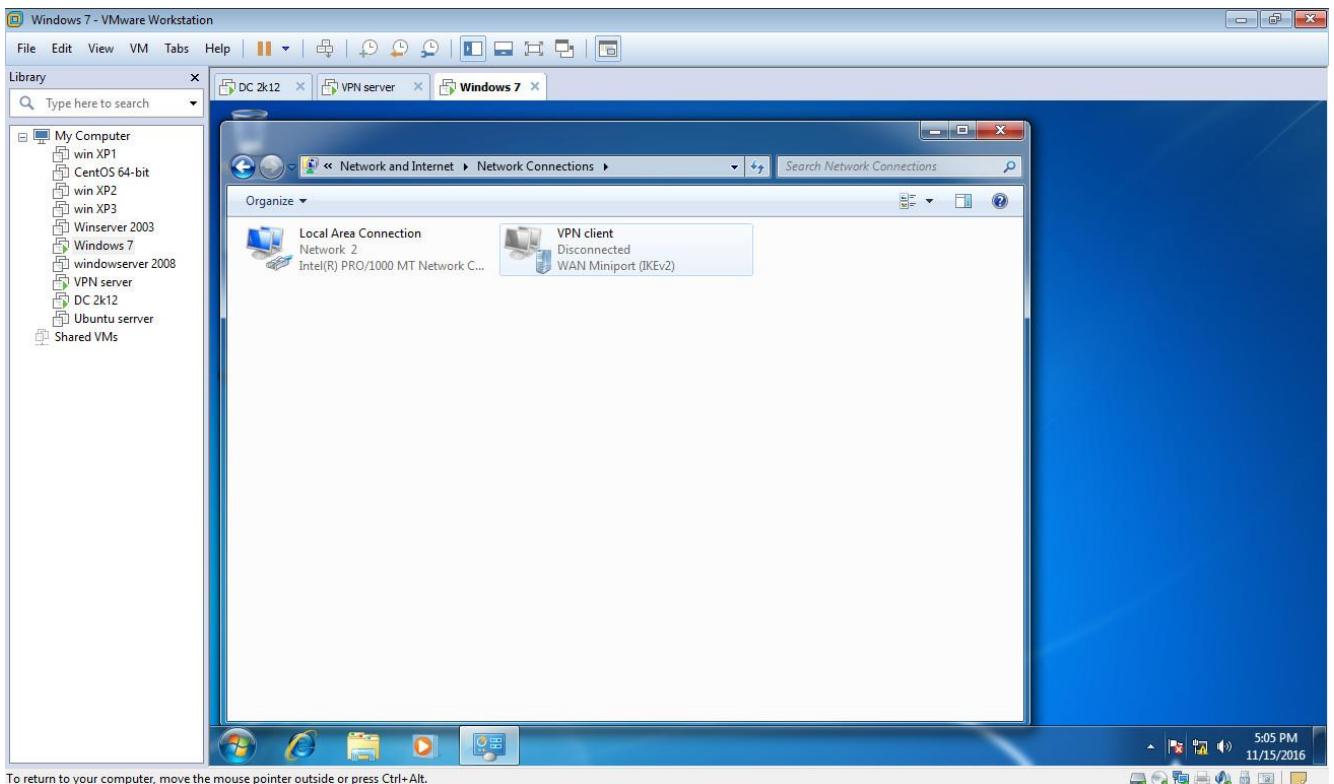
Điền user name, password, domain như đã tạo trước đó ở máy DC sau đó chọn Create. (tick chọn Remember this password để ghi nhớ mật khẩu)



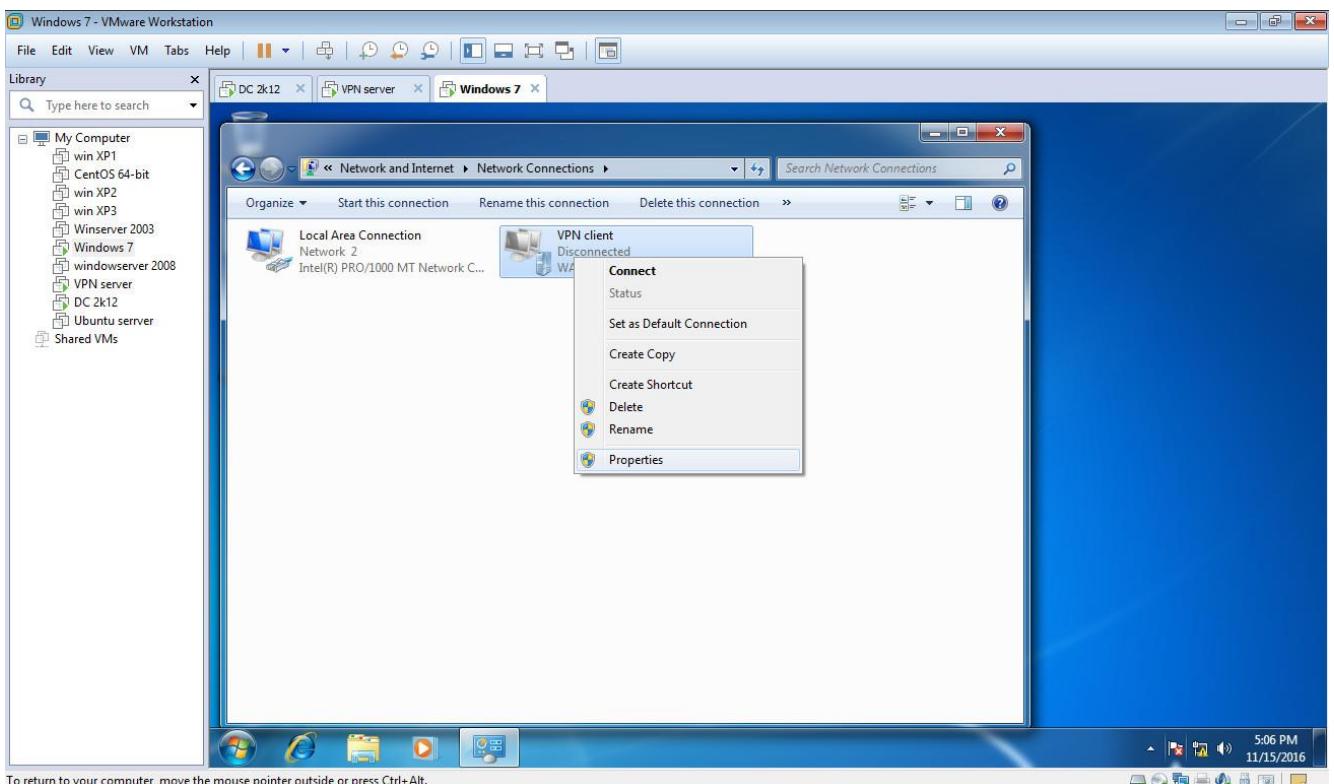
Tạo thành công, click Close để kết thúc



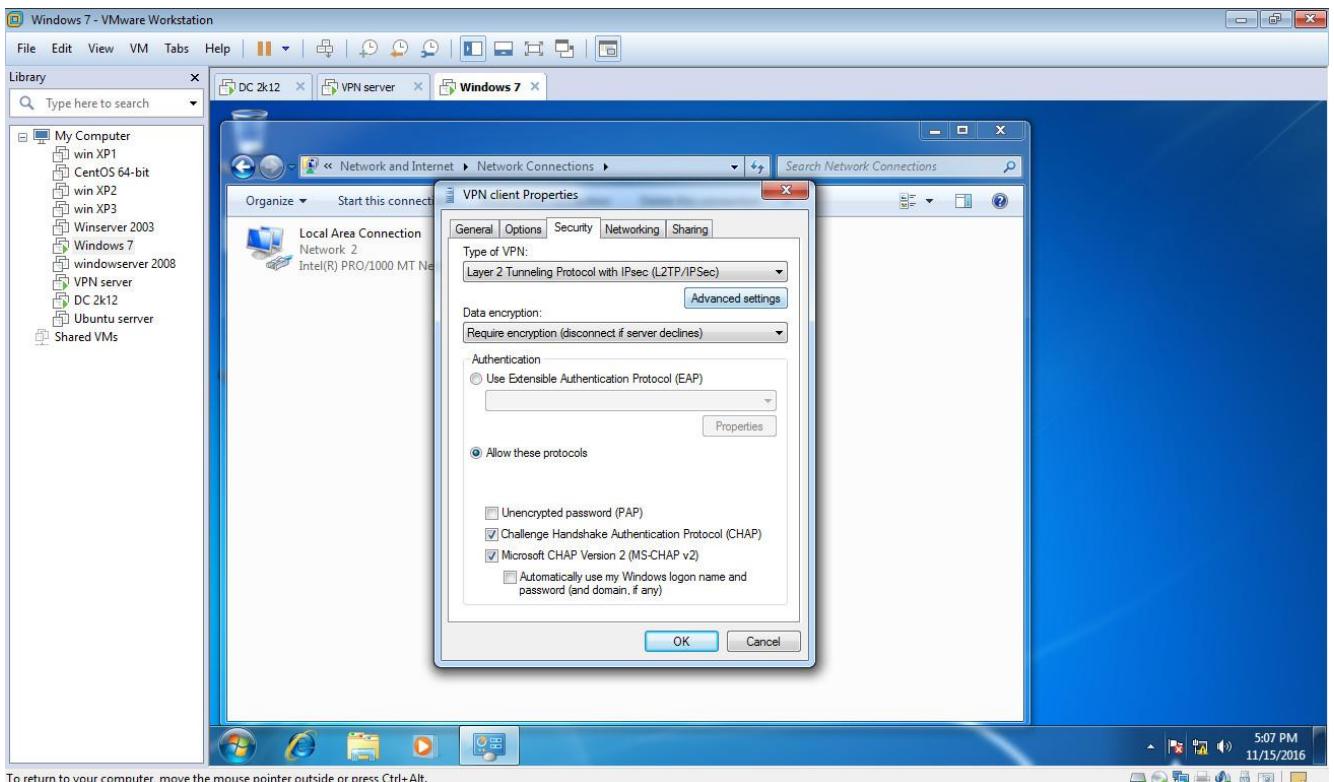
Vào Network connection ta thấy 1 biểu tượng kết nối VPN đã được tạo ra



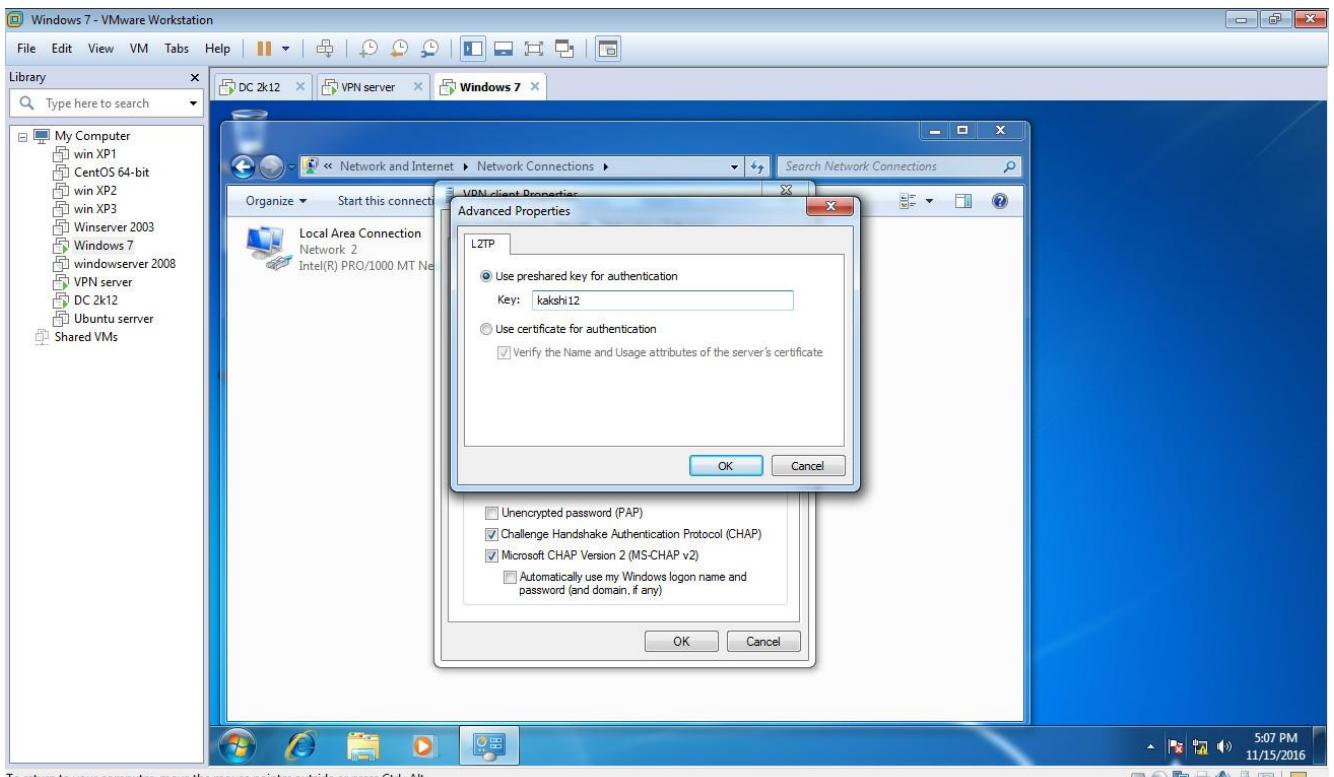
Click chuột phải vào kết nối này và chọn Properties



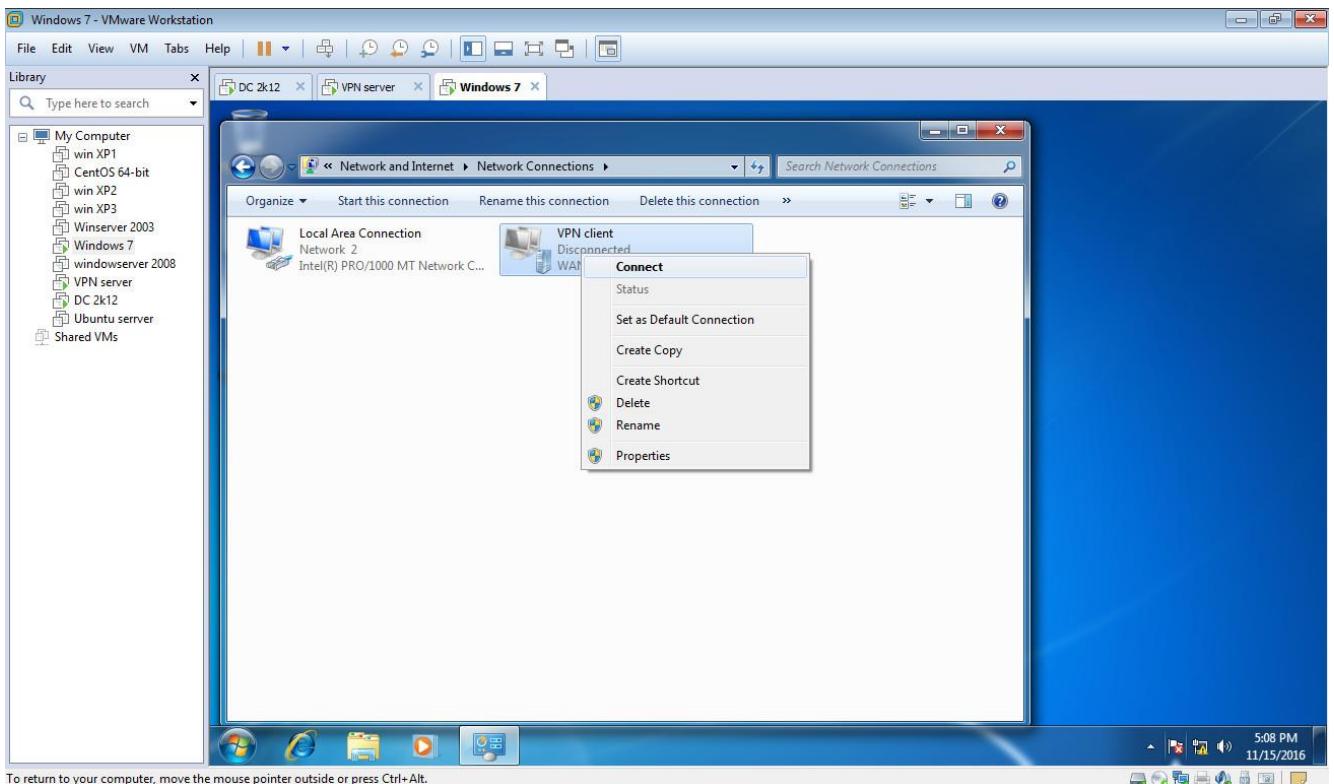
Trên cửa sổ VPN client Properties chọn Tab Security. Tại Type of VPN chọn giao thức Layer 2 Tunneling with IPsec (L2TP/IPSec) sau đó click Advanced Settings



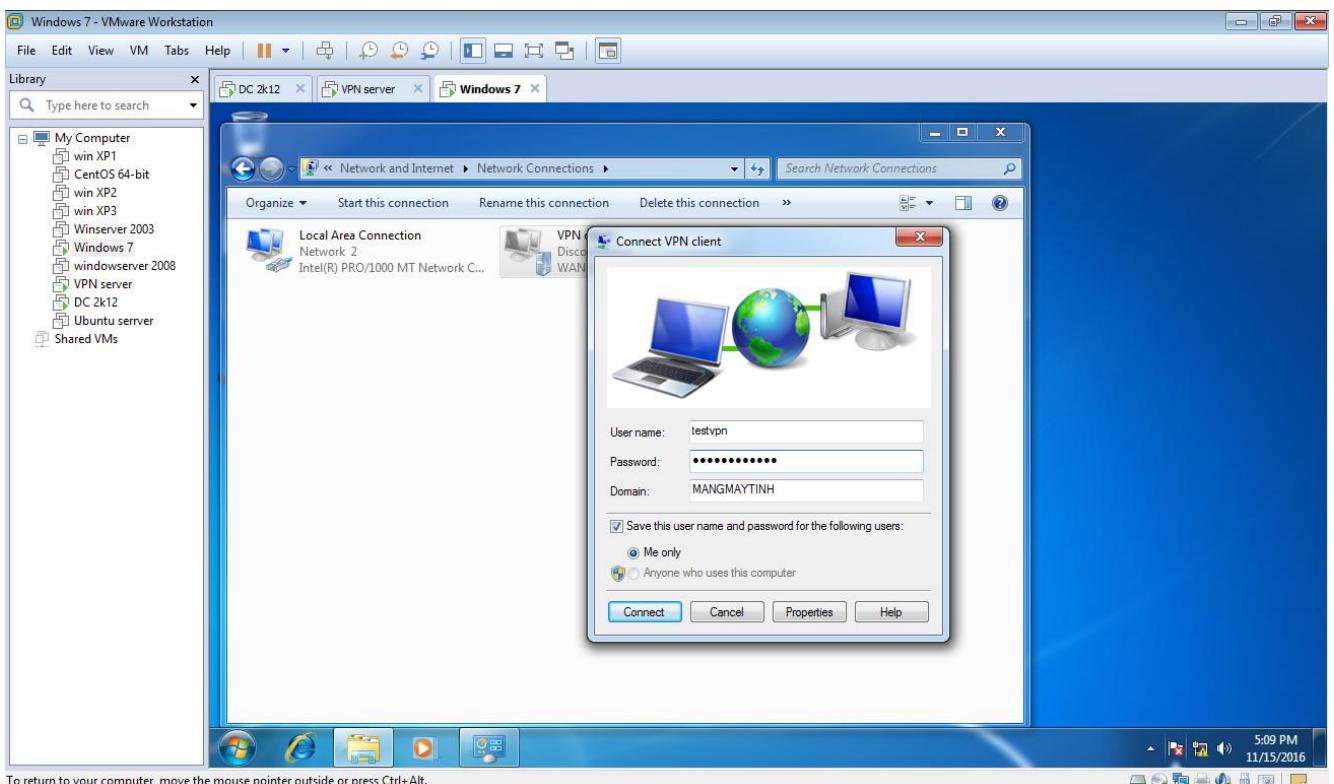
Tick chọn Use preshared key for authentication, gán Key đã tạo trên máy VPNSERVER sau đó click OK



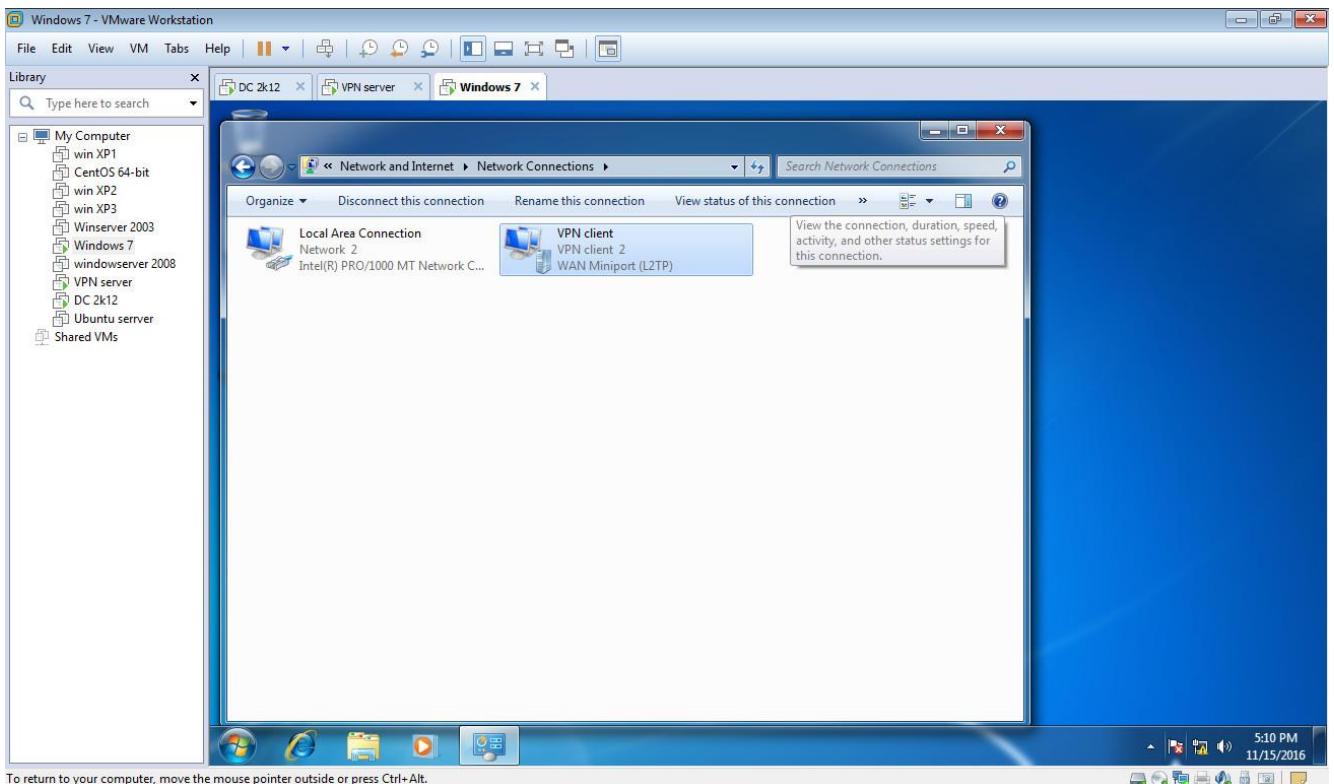
Để kết nối VPN, click chuột phải vào Network VPN vừa tạo chọn Connect



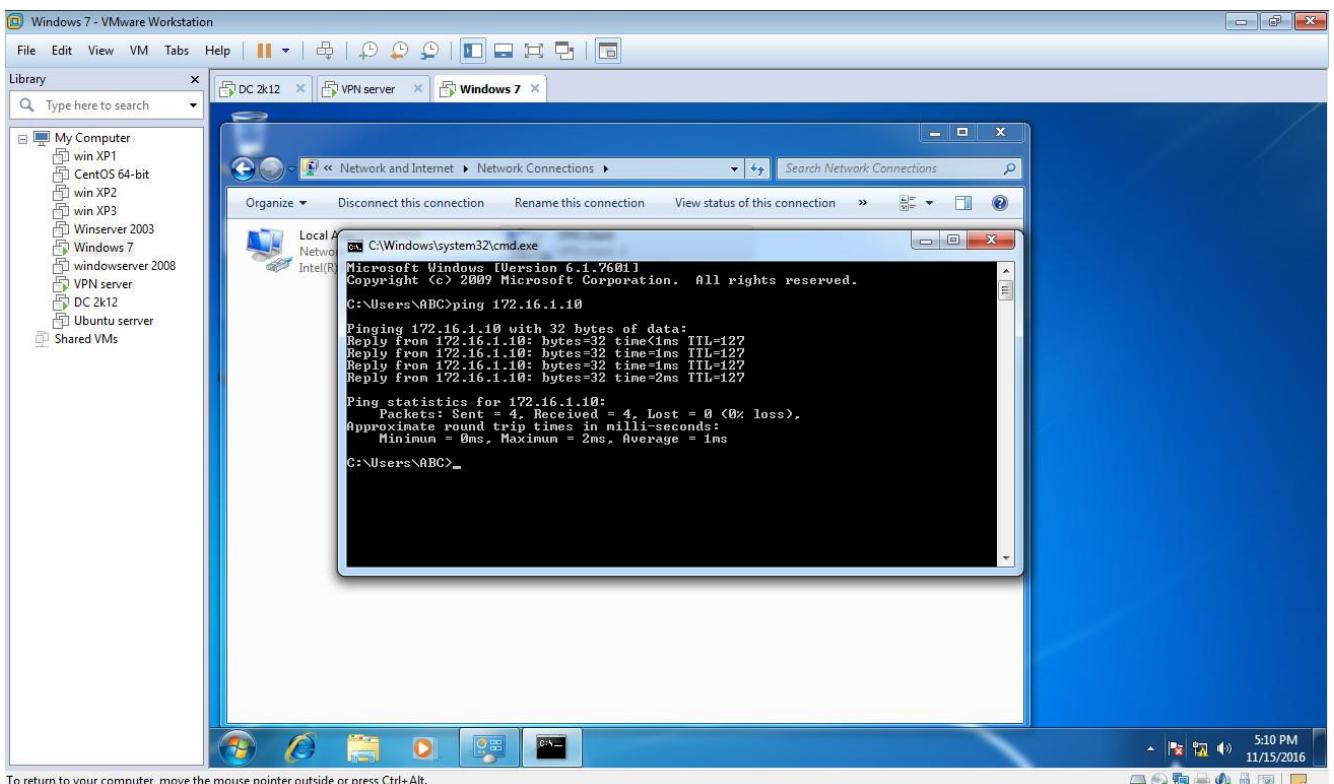
Điền password của user rồi chọn Connect để kết nối



Kết nối VPN thành công với giao thức L2TP



Ping vào máy DC thấy thành công



Muốn ngắt kết nối VPN, click chuột phải chọn Disconnect.

(Nếu gặp lỗi, trên VPN server/ DC tắt firewall với cổng 5000, 4500)